UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Gestão de risco em segurança da informação e privacidade no DNS.PT

Mestrado em Segurança Informática

Ricardo Manuel Sequeira Pires

Trabalho de Projeto orientado por:
Prof.ª Doutora Ana Luísa do Carmo Correia Respício
Dr.ª Carla Inês Machado Esteves

2018

Agradecimentos

Agradeço a todos aqueles que contribuíram, direta ou indiretamente, para o desenvolvimento deste trabalho.

Deixo um especial agradecimento à Professora Ana Respício que sempre me acompanhou e incentivou na realização deste trabalho. O seu empenho, dedicação e apoio na procura de soluções para as questões que se colocaram foram fundamentais para a conclusão do trabalho.

Ao DNS.PT, agradeço reconhecidamente ter permitido o desenvolvimento deste trabalho, e em especial à Dr.ª Inês Esteves a ajuda, acompanhamento e sentido crítico no trabalho desenvolvido e à Dr.ª Sónia Veloso por me motivar todos os dias para atingir os objetivos a que nos propomos.

À minha família, em especial aos meus pais e irmã, pelo apoio incondicional e compreensão.

E ainda, por toda a paciência e apoio demonstrado durante esta jornada agradeço à minha namorada.

Resumo

A evolução tecnológica permitiu um enorme progresso nas sociedades atuais, com inequívocos benefícios na vida moderna, em áreas tão diferentes, como a saúde, a educação, a segurança e o bem-estar económico. A evolução tecnológica levanta, no entanto, novas preocupações e desafios, nomeadamente ao nível da proteção da privacidade dos cidadãos a qual pode ser severamente comprometida por práticas abusivas de recolha, tratamento e utilização de dados pessoais.

Para reforçar a coerência e a efetiva defesa dos direitos e das liberdades fundamentais dos titulares de dados pessoais foi assegurada uma verdadeira harmonização legislativa entre todos os Estados-Membros através da adoção do Regulamento Geral de Proteção de Dados (RGPD), 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Este novo quadro legislativo surge com o objetivo de proteger a privacidade das pessoas singulares através da criação de novas obrigações no tratamento de dados pessoais.

Este novo regulamento sugere, em particular no n.º 1 do artigo 35.º, a avaliação de impacto na privacidade sempre que exista um tratamento "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares", não estabelecendo, contudo, um processo formal para a sua concretização, indicando apenas alguns princípios enformadores para a sua realização.

É sob este enquadramento que se construiu um modelo para gestão do risco em segurança da informação e privacidade para o contexto da Associação DNS.PT, a entidade responsável pela gestão, registo e manutenção do domínio de topo de Portugal .PT. Foi ainda desenvolvido um protótipo aplicacional para assegurar, por um lado, a aplicação das melhores práticas no .PT quanto ao tratamento dos dados pessoais como também à conformidade com o RGPD.

Palavras-chave: Risco, Gestão do Risco, Segurança da Informação, Privacidade, Regulamento Geral de Proteção de Dados

Abstract

The technological evolution has allowed tremendous progress in today's societies, with unequivocal benefits in modern life, in such different areas as health, education, security and economy. However, this evolution raises new concerns and challenges, particularly in terms of protecting citizens' privacy, which can be severely compromised by abusive collection, processing and use of personal data.

In order to strengthen the coherence and effective protection of the rights and fundamental freedoms of personal data holders, a genuine legislative harmonization between all Member States was ensured through the adoption of the General Data Protection Regulation (GDPR), 2016/679 of the European Parliament and of the Council of 27 April 2016. This new legislative framework arises with the aim of protecting the privacy of natural persons by creating new obligations in the processing of personal data.

This new regulation suggests, in particular in number 1 of article 35, the impact's assessment on privacy whenever personal data processing is "likely to involve a high risk to the rights and freedoms of natural persons", but does not establish a formal process for its implementation, indicating only a few principles for its realization.

It is under this environment, that a model for information security and privacy risk management was developed for the context of DNS.PT, the entity responsible for the management, registration and maintenance of the Top-Level-Domain for Portugal .PT. An application prototype was developed to ensure, on one hand, the application of best practices in DNS.PT regarding the processing of personal data as well as the compliance with GDPR.

Keywords: Information Security Risk, Risk Management, Information Security, Privacy, General Data Protection Regulation

Conteúdo

Índice de Figuras

Índice de Tabelas

Capítulo 1

Introdução

1.1 Motivação

A Internet tornou-se parte integrante das nossas vidas, introduziu tecnologias como o e-mail, as redes sociais e os motores de busca no nosso dia-a-dia e, a pouco e pouco, revolucionou a forma como aprendemos, comunicamos e nos relacionamos uns com os outros. Atualmente a Internet desempenha um fator decisivo para o crescimento económico e para o crescimento do emprego, sendo que as cidades inteligentes, a indústria 4.0, ou mesmo a internet das coisas fazem parte de uma realidade próxima. No entanto, estas mesmas tecnologias, criam novas ameaças e desafios ao direito à privacidade dos cidadãos, na medida em que permitem uma vigilância omnipresente dos hábitos de consumo, do que fazemos, com quem nos relacionamos e a partir desta informação extrapolar perfis diferenciadores, essenciais para influenciar decisões políticas, económicas e sociais.

Estas preocupações levaram a União Europeia (EU) a introduzir recentemente novas regras para proteger a privacidade dos cidadãos Europeus com o Regulamento Geral de Proteção de Dados, 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD, 2016). Ainda que esta matéria não seja propriamente uma novidade, este novo quadro legislativo endereça inúmeros desafios às organizações ao nível da sua concretização e operacionalização, exigindo uma abordagem mais robusta e coerente à efetiva proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados, a qual pressupõe o alinhamento de políticas, procedimentos e tecnologia, incluindo a definição um modelo de gestão dos riscos associados ao tratamento de dados pessoais.

A gestão dos riscos da privacidade torna-se obrigatória sempre que existem tratamentos de dados “suscetíveis de implicar um elevado risco para os direitos e

liberdades das pessoas singulares", nomeadamente, quando existe definição de perfis de utilizadores que permitem prever a situação económica, preferências e interesses pessoais dos titulares dos dados, como também quando existe o tratamento de dados pessoais sensíveis em grande escala (art.º 35.º do RGPD, 2016). Nesta perspetiva a adoção de "uma metodologia de gestão de riscos é a forma mais segura de garantir a objetividade e relevância das decisões a tomar no processamento de dados pessoais" (CNIL, 2012).

No contexto de um *Top-Level Domain* (TLD), em particular num *Country Code Top-Level Domain* (ccTLD), onde se enquadra o DNS.PT, doravante .PT, a entidade responsável em Portugal pela gestão, registo e manutenção do domínio de topo de Portugal .PT, requere o tratamento de dados pessoais, quer seja, dos seus clientes e parceiros nas atividades de registo e transferência de nomes de domínio ou ainda dos dados pessoais dos seus colaboradores na gestão dos recursos humanos.

Sob este desígnio o .PT consagra estas preocupações nos seus estatutos, com o comprometimento de manutenção dos níveis de qualidade, fiabilidade e segurança na gestão do ccTLD .PT (DNS.PT, 2013a) e ainda adota um sistema integrado para a gestão da qualidade e segurança informação, no sentido de melhor entender e satisfazer as necessidades dos seus clientes, parceiros e colaboradores assim como para manter a segurança da informação dos mesmos, e ainda antever e adaptar-se às novas ameaças de forma contínua. O .PT é certificado nas normas internacionais ISO/IEC 9001:2015 e ISO/IEC 27001:2013, desde 2013 e 2015 respetivamente, sendo as suas atividades sustentadas pelo Sistema de Gestão de Qualidade e Segurança da Informação (SGQSI), onde se incorporam as atividades referentes à gestão do risco (DNS.PT, 2016).

A necessidade de adoção de um modelo para a gestão do risco em segurança da informação e privacidade e do desenvolvimento de uma aplicação que lhe desse suporte surge no contexto do .PT, mais propriamente no departamento de gestão e administração, pelas novas obrigações consideradas no RGPD, nomeadamente, na necessidade de avaliação de impacto à privacidade dos dados, disposto no artigo 35.º (RGPD, 2016), que até então não estava considerado no sistema implementado na organização.

1.2 Objetivos

Este trabalho teve por objetivo o desenvolvimento de um modelo para a gestão de risco em segurança da informação e privacidade, que considere os requisitos dispostos no RGPD, em particular os dispostos no art.º 35.º deste mesmo regulamento para o contexto do .PT. Este modelo deve ser desenhado considerando o processo de gestão de risco implementado na organização e as práticas e normativos desenvolvidas por entidades de relevo nas matérias de gestão do risco e de proteção de dados pessoais.

O trabalho teve também como objetivo a validação do modelo desenhado através do desenvolvimento de uma aplicação de suporte e do seu teste no contexto do .PT.

1.3 Contribuições

Com o presente trabalho estudou-se o estado de arte das normas e metodologias aceites no âmbito da gestão do risco em segurança da informação e privacidade de dados pessoais, que contribuiu para o desenvolvimento de um modelo e de um processo para a gestão do risco em segurança da informação e privacidade para o contexto do .PT.

O modelo para a gestão do risco em segurança da informação e privacidade foi sustentado pelo desenvolvimento de um protótipo aplicacional que apoia a .PT na identificação, análise, avaliação e tratamento dos riscos da privacidade, tendo em conta os requisitos do RGPD e as boas práticas adotadas internacionalmente.

1.4 Organização do documento

Este documento está organizado da seguinte forma:

- **Capítulo 2 – Conceitos e trabalho relacionado -** Neste capítulo são apresentados alguns conceitos fundamentais relacionados, são estudadas normas, regulamentos e outros trabalhos relevantes para a segurança da informação e para a proteção de dados pessoais;
- **Capítulo 3 – O contexto do DNS.PT -** É apresentado o contexto da Associação DNS.PT, o seu processo e metodologia para gestão do risco e ainda o seu sistema para gestão dos mesmos;

- **Capitulo 4 – Gestão do risco em segurança da informação e privacidade no .PT -** Neste capítulo é apresentado o modelo conceptualizado para a gestão dos riscos em segurança da informação e privacidade de acordo com os requisitos identificados anteriormente e ainda o processo que permitiu a aplicação do mesmo no contexto da Associação DNS.PT.
- **Capitulo 5 – Aplicação para gestão do risco em segurança da informação e privacidade no .PT –** Neste capítulo é apresentada arquitetura da aplicação desenvolvida para suportar o processo para a gestão dos riscos em segurança da informação e privacidade. São também apresentados os resultados dos testes efetuados à aplicação desenvolvida.
- **Capítulo 6 – Conclusão e Trabalho futuro –** Neste capítulo são apresentadas as considerações finais, da análise de todo o trabalho, sendo igualmente propostas algumas melhorias a considerar no futuro.

Capítulo 2

Conceitos e trabalho relacionado

Este capítulo introduz os conceitos fundamentais ao desenvolvimento deste trabalho e que permitem entender o contexto do problema. É apresentada uma reflexão sobre o conceito de privacidade e de dado pessoal, e ainda sobre o conceito de risco, as normas e metodologias internacionais de referência para a gestão de risco e a relação do mesmo com o conceito de privacidade.

2.1 Privacidade

O conceito de privacidade tem a sua génese de acordo com os autores Smith e Shao (2007) na obra "A Política". Esta obra, escrita pelo filósofo grego Aristóteles, datada do ano de 350 A.C. aproximadamente, distingue a esfera pública e das suas atividades políticas da cidade (*polis*) da esfera privada do agregado familiar e da sua vida doméstica (*oikos*).

Apesar do conceito parecer bastante intuitivo, o conceito de privacidade é abstrato e o seu significado e valorização depende de pessoa para pessoa. O que um individuo considera invasão de privacidade, outro pode simplesmente considerar como um ato normal e aceitável.

Não existe uma definição única de privacidade, mas um conjunto de noções. Estas noções de privacidade e da sua proteção têm variado ao longo dos anos nas diferentes nações, culturas e períodos históricos (Venier, 2010). "O direito a ficar sozinho" é a noção de privacidade, apresentada por Warren e Brandeis (1890), atualmente mais consensual. Estes mesmos autores afirmam ainda que "o direito à privacidade acaba quando existe a publicação dos factos pelo seu titular ou com o seu consentimento".

O direito à privacidade foi desde cedo introduzido como uma preocupação da UE, pelo que todos os Estados-Membros são signatários da Convenção Europeia dos

Direitos do Humanos (CEDH). Na CEDH, adotada em 1950, está consignado o direito ao respeito pela vida privada e familiar, no n.º 1 do art.º 8.º onde se lê "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência" (Tribunal Europeu dos Direitos Humanos, 1950).

Em Portugal, o direito à privacidade foi consagrado, ainda de forma pioneira em 1976, no art.º 35.º da Constituição da República Portuguesa (CRP), onde estava acautelada a proteção dos dados pessoais em relação ao uso das novas tecnologias. Atente-se ao n.º 3 do artigo supra referido: " [a] informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis" (*CRP*, 2005).

2.2 Dados pessoais

Na sociedade da informação em que vivemos, a proteção da privacidade passa definitivamente pelo direito a controlar o fluxo da sua informação pessoal e as suas utilizações (Elgesiem, 1996). É nesta perspetiva que é fundamental perceber o que compreende dado pessoal.

O conceito de informação pessoal ou dado pessoal, de acordo com art.º 2.º da diretiva Europeia 95/46/CE de 1995, define-se pelo "conjunto de elementos que levam à identificação de uma pessoa, como o nome, apelido, morada, data de nascimento, ou ainda outros elementos que façam referência a elementos identificadores da identidade física, fisiológica, psíquica, económica, cultural ou social, a voz e a imagem da pessoa". Podemos ainda considerar, pelo art.º 8.º desta mesma diretiva, a existência de uma categoria especial de dados pessoais, os dados pessoais sensíveis. Os dados pessoais sensíveis são aqueles que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual".

No contexto português, a Lei da Proteção de Dados Pessoais (LPDP), lei n.º 67/98 (1998), que transpôs para a Ordem Jurídica Portuguesa, a diretiva 95/46/CE (1995), manteve-se a mesma definição de dado pessoal, contudo, com uma novidade, o dado pessoal poderia estar sobre qualquer formato incluindo imagem e som.

Na nova regulamentação Europeia que revoga a anterior lei nº 67/98 (1998), o RGPD, em linha com as anteriores definições, dispõe no art.º 4.º, que dado pessoal corresponde a uma "informação relativa a uma pessoa singular identificada ou identificável, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (RGPD, 2016).

2.3 Proteção dos dados pessoais

No contexto tecnológico atual observa-se com maior frequência e em maior volume o tratamento de dados pessoais, isto é, de acordo com o disposto n.º 2 do artigo 4.º do RGPD, "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". O tratamento destes dados causa grandes preocupações pois, permite com a capacidade tecnológica atual, com alguma facilidade extrapolar tendências, movimentos, interesses e atividades de indivíduos e de grupos e tomar decisões de acordo com estas informações.

No entanto, esta preocupação já era tida pela Organização para a Cooperação e Desenvolvimento Económico (OCDE), quando desenvolveu e publicou um guia para nortear a proteção dos dados pessoais que, apesar de não vinculativo, veio reconhecer que a proteção da privacidade era uma prioridade na política internacional (OCDE, 1980). No guia elaborado são elencados os princípios fundamentais da proteção dos dados pessoais como a:

- **Limitação da recolha**: todos os dados pessoais recolhidos devem ser obtidos através de meios justos, e se apropriado com o conhecimento e consentimento do titular dos dados.
- **Qualidade dos dados**: os dados pessoais devem ser precisos, completos e mantidos atualizados para o propósito que foram recolhidos.

- **Limitação da finalidade**: o propósito da recolha de dados pessoais deve ser especificado no momento da sua recolha.
- **Limitação da utilização**: os dados pessoais recolhidos não devem ser divulgados, disponibilizados ou usados para outros fins que não os especificados.
- **Segurança da informação**: os dados pessoais devem ser protegidos por controlos de segurança razoáveis contra riscos como a perda, acesso não autorizado, destruição ou divulgação.
- **Transparência**: devem ser definidas políticas para a utilização de dados pessoais.
- **Direito ao Acesso, Eliminação e Retificação**: o titular dos dados pessoais, tem o direito de saber que dados os controladores possuem sobre os mesmos dentro de um prazo razoável, e solicitar o seu apagamento ou retificação.
- **Responsabilidade**: o controlador é responsável por cumprir com as medidas anteriores.

Em 2016, surge o novo regulamento europeu para a proteção de dados, o RGPD. Neste são consideradas todas as organizações, independentemente do seu tamanho ou volume de negócios, sempre que efetuem o tratamento dados pessoais de cidadãos da UE ou de cidadãos não europeus que estejam ou tenham estado na UE e cujos dados tenham sido recolhidos pelas referidas empresas, ainda que o tratamento dos mesmos ocorra fora da UE. Em linha com o guia publicado pela OCDE em 1980, o RGPD adota também os princípios da licitude, lealdade, transparência, da limitação das finalidades, da minimização dos dados, da exatidão, da limitação da conservação, da segurança da informação e da responsabilização (OCDE, 1980). No RGPD são reconhecidos os direitos aos cidadãos da UE descritos na Tabela 1. Os direitos concedidos configuram assim requisitos obrigatórios a qualquer negócio que efetue o tratamento de dados pessoais.

Tabela 1 – Quadro resumo dos direitos consagrados aos titulares dos dados no RGPD.

Artigo	Direito	Descrição
13.º e 14.º	Direito à informação	Os titulares dos dados têm o direito a serem informados da recolha e utilização dos seus dados pessoais. É fundamental para a transparência que o propósito do tratamento dos dados, os tempos de retenção e com quem vai ser partilhada seja dada a conhecer ao titular. A informação ao titular deve ser dada de forma concisa, transparente, acessível e utilizar uma linguagem simples.
15.º	Direito ao acesso	Os titulares dos dados têm o direito a ter acesso à sua informação pessoal e dados suplementares. O titular deve ter uma resposta ao seu pedido de acesso no prazo máximo de um mês.
16.º e 19.º	Direito à retificação	Os titulares dos dados têm o direito a solicitar a retificação dos seus dados pessoais. O titular deve ter uma resposta ao seu pedido de retificação no prazo máximo de um mês.
17.º e 19.º	Direito ao esquecimento	Os titulares dos dados têm o direito a solicitar a remoção dos seus dados pessoais. O titular deve ter uma resposta ao seu pedido de remoção no prazo máximo de um mês.
18.º e 19.º	Direito à limitação da finalidade	Os titulares dos dados têm o direito a solicitar a restrição ou supressão do tratamento dos dados. O titular deve ter uma resposta ao seu pedido no prazo máximo de um mês.
20º	Direito à portabilidade	Os titulares dos dados têm o direito a solicitar a portabilidade dos seus dados para um outro serviço. Isto permite aos titulares mover, copiar ou transferir dados pessoais de um ambiente informático para outro de forma segura e sem obstáculos à usabilidade. O titular deve ter uma resposta ao seu pedido no prazo máximo de um mês.
21º	Direito à oposição	Os titulares dos dados têm o direito a se oporem ao tratamento dos seus dados pessoais com base no legítimo interesse, a campanhas diretas de marketing e a tratamentos para fins científicos e/ou históricos e estatísticos.
22º	Direito à não sujeição a decisões individuais automatizadas	Os titulares dos dados têm o direito a não ser sujeito a decisões automatizadas, que produza efeitos na sua esfera jurídica ou que o possa afetar de forma significativa.

2.4 Sistema de gestão de segurança da informação

Com a evolução tecnológica, os ambientes de negócio ficaram globalmente interligados e consequentemente mais expostos às ameaças do ciberespaço. Neste contexto, foi necessário às organizações adotarem mecanismos para uma melhor gestão da segurança da informação, que permitissem proteger de forma continuada a confidencialidade, integridade e disponibilidade dos seus ativos. Considera-se um ativo a proteger algo que represente valor para a organização como por exemplo, um servidor físico, uma *pen/usb* com dados sensíveis ou mesmo um serviço que é disponibilizado ao público em geral.

A ISO/IEC 27001:2013, é uma norma reconhecida internacionalmente, publicada em 2013, que define o estabelecimento de um sistema de gestão de segurança da informação (SGSI) orientado ao risco, que se adapta à estrutura e dimensão da organização e requere a definição de políticas, procedimentos, práticas e de recursos (ISO, 2017). As organizações têm vindo a adotar este sistema, com o objetivo garantir a segurança da informação e de dar garantias de confiança aos seus clientes e parceiros, conforme podemos observar pelo crescimento do número de certificações ilustrado na Figura 1.

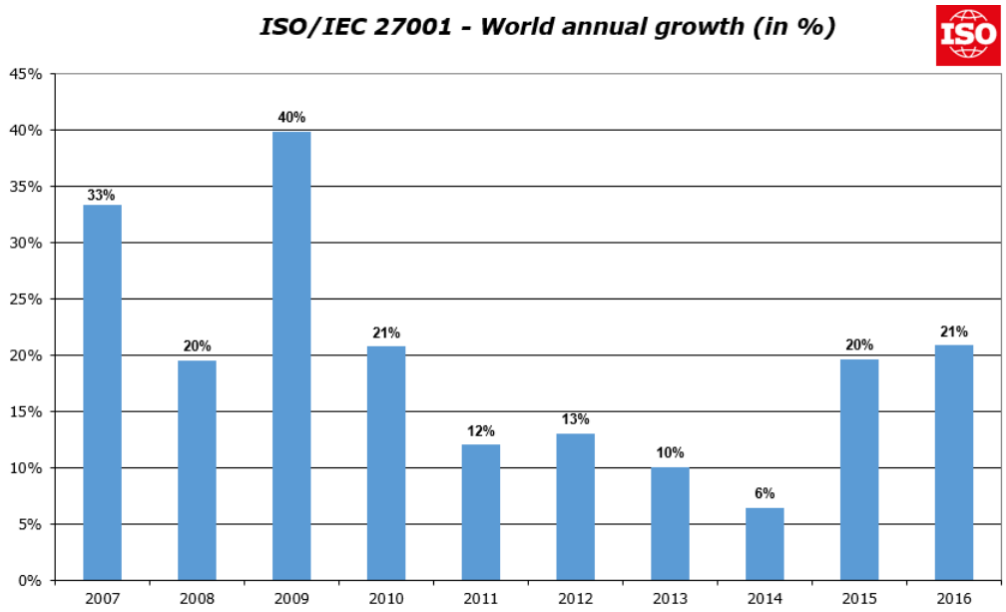

Figura 1 – Taxa de crescimento anual do número de certificações ISO/IEC 27001. Extraído de (ISO, 2017).

O SGSI abrange de modo holístico todas as atividades das organizações, e tem por objetivo estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a

segurança da informação, adotando na sua base o ciclo Planear-Desenvolver-Verificar-Agir[1] (PDCA). A implementação de um SGSI implica o envolvimento de todas as áreas funcionais do negócio, sendo esperado a definição de:

1. **Contexto da Organização**: é necessário compreender a organização e o seu contexto assim como as questões internas e externas relevantes para a sua missão e expectativas das partes interessadas. Neste ponto deve estar definido o âmbito do SGSI a estabelecer;
2. **Liderança**: é necessário definir as responsabilidades na gestão do SGSI e assegurar o comprometido da gestão de topo com as mesmas. A política de segurança da informação deve estar alinhada com os objetivos e a estratégia do negócio;
3. **Planeamento**: é necessário identificar e efetuar o tratamento dos riscos e as oportunidades, assim como a definição de objetivos e métricas que possibilitem a avaliação da melhoria do SGSI. Deve assim ser implementado um processo de gestão de risco, onde sejam incluídas a atividades de apreciação e tratamento dos riscos;
4. **Suporte**: é necessário a organização assegurar a disponibilização de recursos necessários à implementação, manutenção e melhoria contínua do SGSI. Entre os recursos necessários, estão a determinação contínua das competências existentes no seio da organização e na sensibilização das pessoas para as questões relacionadas com o SGSI, como, por exemplo, as políticas de segurança da informação;
5. **Operação**: é necessário implementar processos e procedimentos de planeamento e controlo operacional, de modo a garantir o cumprimento dos requisitos de segurança. Aplicar medidas de controlo para as alterações planeadas e rever as implicações das alterações não planeadas e aplicar medidas corretivas;
6. **Avaliação do Desempenho**: é necessário a organização monitorizar, medir, analisar e avaliar o desempenho e a eficácia do SGSI. Para avaliar o desempenho do SGSI e se este continua a responder aos requisitos da norma, devem ser realizadas auditorias internas. Deve ainda ser realizada uma revisão pela gestão dos resultados obtidos apontado para possíveis melhorias ao SGSI;

[1] Plan-Do-Check-Act na literatura anglo-saxónica.

7. **Melhoria**: é necessário de forma contínua avaliar as não conformidades identificadas e implementar medidas corretivas para as mitigar ou eliminar para que não se repitam.

A norma ISO/IEC 27001:2013 divide-se em 14 domínios, constituídos por 35 objetivos de controlo e 114 controlos (ISO/IEC, 2013). Esta norma toca as mais diversas temáticas da segurança da informação, desde a governação com a definição de políticas da segurança da informação, ao cumprimento das obrigações legais nas matérias da segurança da informação e ainda da privacidade. As preocupações com a proteção de dados pessoais, fazem assim, também parte da ISO/IEC 27001:2013, através do disposto no controlo A.18.1.4 – Privacidade e proteção de dados pessoais.

2.5 Risco e a sua gestão

A noção do risco segundo dicionário da língua portuguesa é a "possibilidade de um acontecimento futuro e incerto; perigo" (Porto Editora, 2018). De acordo com a norma NP ISO 31000:2009, o risco é o efeito de incerteza (positivo ou negativo) na consecução dos objetivos. Segundo esta norma, entende-se ainda que os efeitos causados pela materialização da incerteza na consecução dos objetivos se denominam de consequência e as causas que podem levar a sua consecução por fontes do risco (ISO, 2013).

A noção de risco foi se modificando ao longo do tempo, deixando de estar apenas associada a consequências negativas e tornando-se também associada a consequências positivas. É, no entanto, comum associar-se consequências negativas a riscos e consequências positivas a oportunidades (McNamee, 1998).

Os riscos podem ainda ser classificados como exógenos ou endógenos, sendo que os riscos endógenos são aqueles que podemos controlar e os exógenos aqueles que não podemos controlar, como por exemplo os desastres naturais (Hull, 1992). Ainda o mesmo autor afirma que o risco resulta da combinação de uma incerteza e de uma consequência. Ainda refere que quando isolados os fatores da consequência e da incerteza não se verificam situações de risco, isto é, a incerteza sem consequência não resulta num risco, como também a consequência sem a incerteza.

Podemos expressar o risco pela combinação dos fatores da consequência de um evento, doravante designado por impacto, pela incerteza da ocorrência, doravante designado por verosimilhança.

$$Risco = Impacto * Verosimilhança$$

A redução do risco é conseguida através da implementação de controlos. Controlos são medidas como, por exemplo, a implementação de processos, políticas ou práticas nas organizações que resultem na modificação do nível de risco (ISO, 2013).

Ao resultado da aplicação de controlos sobre o risco denominamos de risco residual. De forma abstrata podemos expressar este risco pela subtração ao risco do risco mitigado pelos controlos (Whitman e Mattord, 2014):

$$Risco\ Residual = Risco * (1 - porção\ mitigada\ por\ controlos)$$

A norma internacional, na versão portuguesa NP ISO 31000:2009 (ISO, 2013), foi desenvolvida pela *International Organization for Standardization* (ISO), e estabelece diretrizes e boas práticas para a gestão de risco. Nesta está reconhecido que todos os tipos de organização enfrentam fatores e influências, internos e externos que tornam incerto quanto ao cumprimento da sua missão e objetivos, ou seja, estão expostos a riscos. A gestão do risco, segundo esta norma, representa um conjunto de "atividades coordenadas para orientar e controlar uma organização no que respeita ao risco", que se iniciam no estabelecimento do contexto, na apreciação do risco, e no tratamento dos riscos. É parte integrante deste processo a comunicação com as partes interessadas, a monitorização e revisão dos riscos, conforme podemos observar na Figura 2.

Uma gestão eficaz do risco, segundo a NP ISO/IEC 31000:2009, considera os seguintes os princípios em todas as suas etapas:

1. A gestão do risco cria e protege o valor;
2. A gestão do risco é parte integrante de todos os processos organizacionais;
3. A gestão do risco é parte da tomada de decisão;
4. A gestão do risco considera explicitamente a incerteza;
5. A gestão do risco é sistemática, estruturada e atempada;
6. A gestão do risco baseia-se na melhor informação disponível;
7. A gestão do risco é feita à medida;

8. A gestão do risco tem em conta fatores humanos e culturais;
9. A gestão do risco é transparente e participada;
10. A gestão do risco é dinâmica, iterativa e reativa à mudança;
11. A gestão do risco facilita a melhoria contínua da organização.

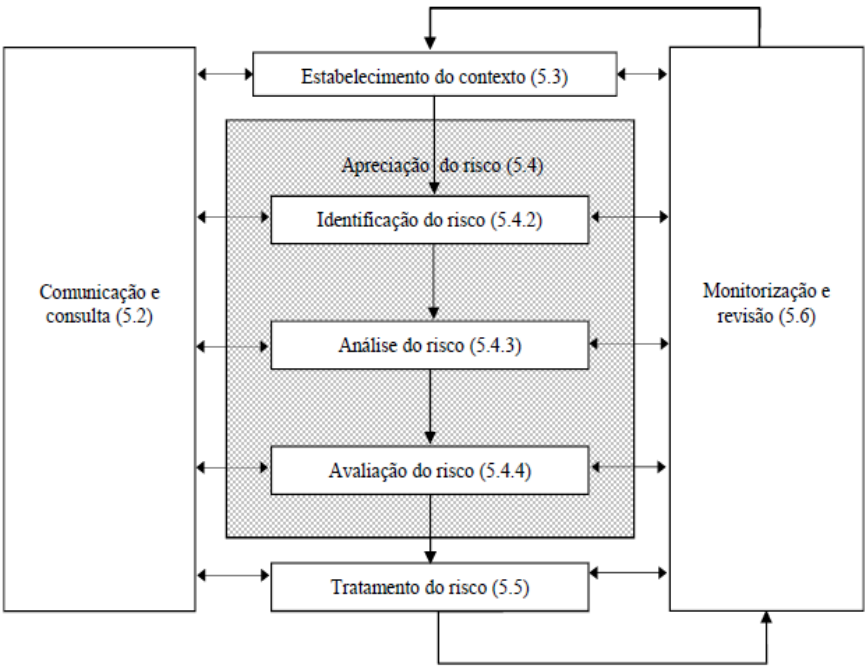

Figura 2 – Processo de gestão de riscos. Extraído de (ISO, 2013).

O processo de gestão de risco conta com a fase da **Comunicação e Consulta** com as partes interessadas quer internas como externas. Esta fase compreende todas as fases do processo de gestão de risco. Numa fase inicial, o plano de consulta e comunicação aborda questões como os riscos e as suas consequências (se conhecidas), assim como as medidas tomadas para os tratar. É essencial nesta fase que todas as partes interessadas e responsáveis pela implementação compreendam os fundamentos das decisões tomadas e as razões para a necessidade das ações. As partes interessadas são fundamentais nesta fase pois produzem juízos sobre o risco baseado na sua perceção. Estas perceções devem ser registadas e identificas, devendo ser consideradas no momento da tomada de decisão.

Na fase seguinte, o **Estabelecimento do Contexto**, pretende-se a definição dos objetivos e dos requisitos das partes interessadas internas e externas assim como os critérios dos riscos a considerar na gestão do risco. No contexto externo da organização importa o estabelecimento dos objetivos tomar em consideração a sua envolvente social,

cultural, político, financeiro, tecnológico, legal e regulamentar aplicado à mesma. No contexto interno o alinhamento à cultura da organização, os processos, a estrutura e a estratégia são os fatores a ter em consideração para a gestão do risco. Tanto as considerações do contexto externo como interno devem ser utilizados para a análise da significância do risco.

Na fase da **Identificação do Risco** devem ser enumeradas de forma exaustiva as fontes dos riscos, as áreas de impacto, eventos, as suas causas e as potencias consequências. É importante identificar nesta fase todas as fontes dos riscos, caso contrário estes não serão incluídos nas fases seguintes. Na identificação dos riscos devem ser envolvidas as pessoas com conhecimento adequado.

Na fase da **Análise do Risco** pretende-se a consideração das causas e fontes do risco, as suas consequências positivas e negativas e a verosimilhança dessas consequências ocorrerem. Devem então ser identificados os fatores que afetam as consequências e a verosimilhança. A combinação da consequência e da verosimilhança resulta no nível do risco que devem ser comunicados aos decisores e, se apropriado, a outras partes interessadas.

Na fase da **Avaliação do Risco** é efetuada a comparação dos resultados obtidos da análise anterior com os critérios do risco identificados na fase do estabelecimento do contexto, e é apoiada a tomada de decisão sobre os riscos que necessitem de tratamento e a sua prioridade de tratamento.

Na fase do **Tratamento do Risco** são selecionadas uma ou mais opções para modificar ou implementar controlos de modo a tratar o risco. Esta fase incluí um ciclo inicial de avaliação onde é apreciado o nível o tratamento do risco, avaliado se o risco residual é tolerável, se não for tolerável deve ser gerado um novo tratamento e por fim é apreciado novamente o tratamento do risco. Existem diversas formas de tratamento do risco que incluem, evitar o risco deixando de prosseguir a atividade, assumir o risco perseguindo uma oportunidade, remover a fonte do risco, alterar a verosimilhança, alterar as consequências, partilhar o risco com uma terceira parte ou reter o risco com base em decisão informada. No final os decisores e partes interessadas deverão estar cientes da natureza e dimensão do risco residual após o tratamento do risco.

A **Monitorização e Revisão** deve ser uma parte planeada do processo de gestão do risco e envolver a verificação de forma periódica ou ad hoc. As responsabilidades pela monitorização e revisão devem ser claramente definidas e devem assegurar que os controlos são eficazes e eficientes quer na conceção como na operação, promover a

melhoria da apreciação do risco, analisar e aprender com os eventos, detetar as alterações no contexto e promover as alterações necessárias e identificar os riscos emergentes.

2.6 Gestão do risco em segurança da informação

Considerando a importância da gestão dos riscos para as organizações, nomeadamente os riscos da segurança da informação, a ISO/IEC 27005:2011 é uma referência nestas matérias (ISO/IEC, 2011a).

A ISO/IEC 27005:2011 estabelece as diretrizes para a gestão de risco em segurança da informação e introduz alguns termos, para além da confidencialidade, integridade e confidencialidade que valem a pena referir:

- **Ameaça**: Causa potencial de um incidente inesperado, que pode resultar em danos para os sistemas ou para a organização;
- **Vulnerabilidade**: Fraqueza de um ativo ou de um controlo que pode ser explorado por uma ou mais ameaças;
- **Evento**: Ocorrência ou alteração num conjunto de pressupostos;
- **Consequência**: Resultado de um evento afetar um objeto;
- **Controlo**: Medida que modifica o risco;
- **Impacto**: Alteração no nível de cumprimento dos objetivos do negócio;
- **Ativo**: Qualquer recurso que tenha valor para a organização.

O processo de gestão de risco na segurança da informação, apresentado na ISO/IEC 27005:2011 e ilustrado na Figura 3, tem por base o ciclo do PDCA. Assim, em cada uma das fases do ciclo, decorrem as seguintes atividades da gestão do risco:

Planear:

- Estabelecer o contexto da gestão de risco da segurança da informação, onde são incluídos os critérios para a abordagem à gestão de riscos, a avaliação do risco, como a determinação do impacto e da verosimilhança, e dos níveis de aceitação do risco. São identificados os ativos envolvidos e quais são incluídos na apreciação do risco. São ainda também definidos o âmbito e os limetes, os papéis e responsabilidades no processo de gestão de risco.

- A análise de risco, inclui a identificação dos riscos de segurança da informação para os ativos, o seu valor, ameaças, controlos aplicados, vulnerabilidades e consequências da sua exploração. Considerando a verosimilhança das vulnerabilidades serem exploradas é calculada a magnitude do risco.
- Desenvolver um plano de tratamento de risco, onde são identificados os controlos para eliminar, mitigar, transferir ou aceitar os riscos. Os controlos devem serem selecionados tendo por base uma análise de custo/benéfico. Os riscos ao serem tratados passam a ser identificados de riscos residuais.
- A aceitação do risco deve ser uma decisão informada, fundamentada nos critérios de aceitação e documentada. Os responsáveis devem rever e aprovar o plano de tratamento de risco.

Desenvolver:

- Implementar as medidas identificadas no plano de tratamento de risco.

Verificar:

- Monitorizar e rever se o contexto da gestão do risco, os ativos identificados em âmbito, os critérios de apreciação e aceitação do risco, os resultados das avaliações de risco se mantêm adequados e consistentes com os objetivos do negócio. Identificar novas ameaças e vulnerabilidades para o negócio.

Agir:

- Manter e melhorar o processo de gestão de risco da segurança da informação.

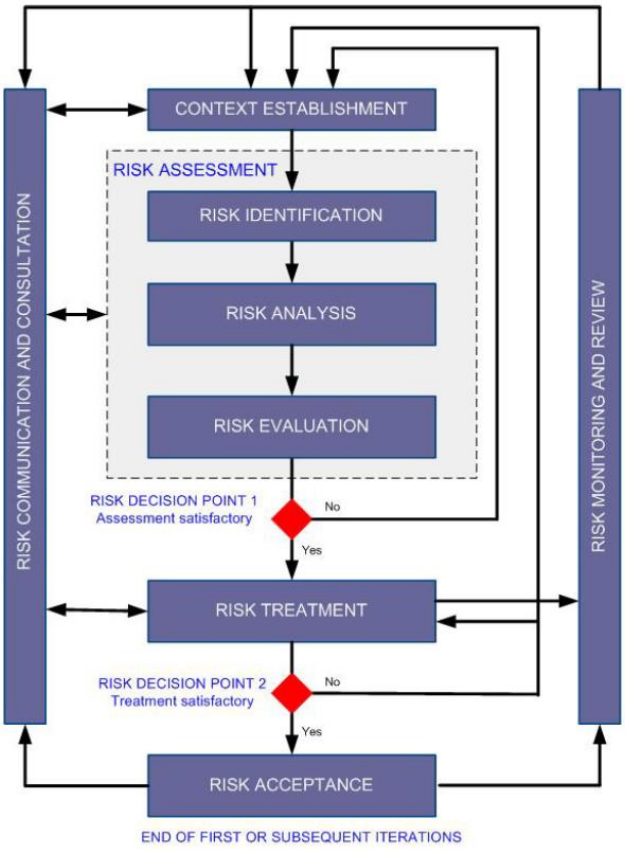

Figura 3 – Processo de gestão do risco. Extraído de (ISO/IEC, 2011a).

2.7 Gestão do risco em privacidade

A avaliação de risco na privacidade ou a avaliação de impacto na privacidade (*Privacy Impact Assessment* – PIA) segundo a norma ISO/IEC 29001:2011 (ISO/IEC, 2011b) é um "processo de identificação, análise e avaliação dos riscos no que diz respeito ao processamento de dados pessoais identificáveis (PII)". Já segundo Stewart (1999), o PIA é "um processo que leva a cabo um esforço consciente e sistemático de avaliação do impacto na proteção dos dados pessoais e das opções que se podem adotar em relação a uma determinada proposta de projeto".

Em 2014, Oetzel e Spiekermann apresentam uma metodologia de avaliação de impacto na privacidade orientada a projetos (Oetzel e Spiekermann, 2014). A metodologia apresentada por estes dois autores é constituída por **sete passos** conforme se ilustra na Figura 4.

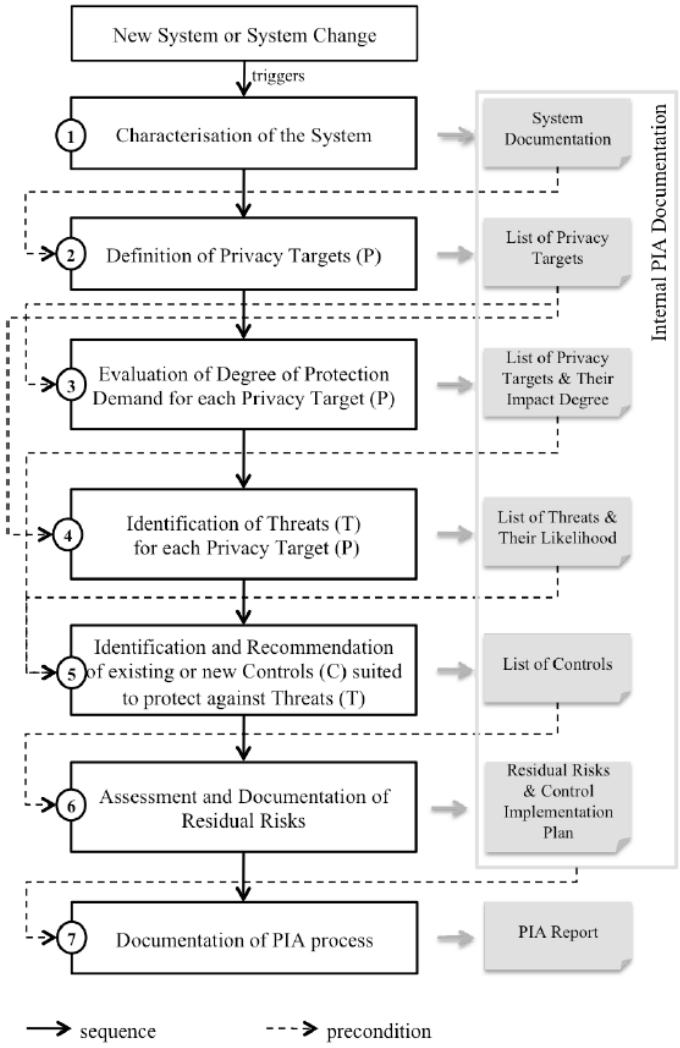

Figura 4 – Processo de avaliação de impacto na privacidade. *Extraído de* (Oetzel e Spiekermann, 2014).

O processo de avaliação do impacto na privacidade, o PIA, tem inicio quando existe um novo sistema ou uma alteração ou atualização a um sistema, e deve ser conduzido em paralelo com o desenvolvimento do sistema. É de referir que segundo o RGPD prevê no n.º 1 do art.º 35.º, uma avaliação de impacto aos dados pessoais só deve ser efetuada quando existir um tratamento "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares".

No **primeiro passo** da metodologia apresentada por Oetzel e Spiekermann é efetuada uma avaliação criteriosa ao sistema, descrevendo os componentes do sistema de forma compreensiva, os processos de negócio envolvidos, aos casos de uso, aos dados processados, fluxo de dados e potenciais problemas para a privacidade.

No **segundo passo**, considerando os princípios de privacidade elencados no art. 2.º da *Diretiva 95/46/CE de 1995* e ainda na proposta do novo regulamento para a proteção de dados europeu (CE (Comissão Europeia), 2012), os autores derivam os

requisitos, ou como os autores denominam “Privacy Targets”, para a privacidade, conforme ilustrado na Figura 5.

Privacy Principles		Privacy Targets
P1 - Data Quality		
	P1.1	Ensuring fair and lawful processing through transparency
	P1.2	Ensuring processing only for legitimate purposes
	P1.3	Providing purpose specification
	P1.4	Ensuring limited processing for specified purpose
	P1.5	Ensuring data avoidance
	P1.6	Ensuring data minimization
	P1.7	Ensuring data quality, accuracy and integrity
	P1.8	Ensuring limited storage
P2 - Processing Legitimacy		
	P2.1	Ensuring legitimacy of personal data processing
	P2.2	Ensuring legitimacy of sensitive personal data processing
P3 - Information Right of Data Subject		
	P3.1	Providing adequate information in cases of direct collection of data from the data subject
	P3.2	Providing adequate information where data has not been obtained directly from the data subject (e.g. from third parties)
P4 - Access Right of Data Subject		
	P4.1	Facilitating the provision of information about processed data and purpose
	P4.2	Facilitating the rectification, erasure or blocking of data
	P4.3	Facilitating the portability of data
	P4.4	Facilitating the notification to third parties about rectification, erasure and blocking of data
P5 - Data Subject's Right to Object		
	P5.1	Facilitating the objection to the processing of personal data
	P5.2	Facilitating the objection to direct marketing activities
	P5.3	Facilitating the objection to disclosure of data to third parties
	P5.4	Facilitating the objection to decisions that are solely based on automated processing of data
	P5.5	Facilitating the data subject’s right to dispute the correctness of machine conclusions
P6 - Security of Data		
	P6.1	Ensuring the confidentiality, integrity and availability of personal data storage, processing and transmission
	P6.2	Ensuring the detection of personal data breaches and their communication to data subjects
P7 - Accountability		
	P7.1	Ensuring the accountability of personal data storage, processing and transmission

Figura 5 – Princípios e requisitos para a privacidade. Extraído de (Oetzel e Spiekermann, 2014).

No **terceiro e quarto passo** da metodologia apresentada por *Oetzel e Spiekermann*, são avaliados cada um dos requisitos de privacidade quanto ao impacto na privacidade e, posteriormente para cada um destes são identificadas as ameaças e a respetiva verosimilhança.

Para mitigar, minimizar ou eliminar as ameaças, os autores no **quinto passo**, sugerem a identificação dos controlos. Os controlos, segundo autores, podem ser de dois tipos: os técnicos, que são incluídos diretamente nos sistemas e os não técnicos que são os relativos à gestão e do foro administrativo.

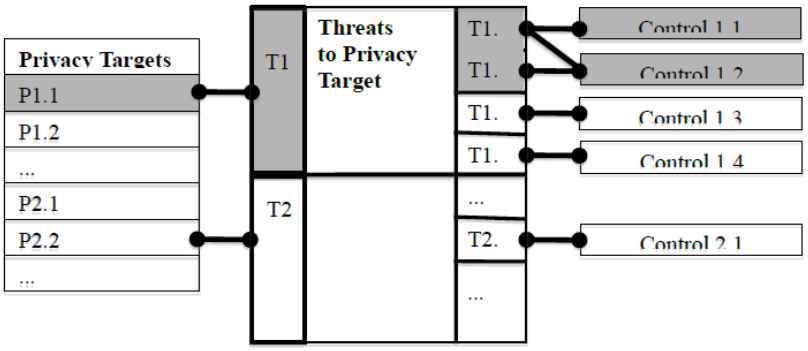

Figura 6 – Mapeamento de requisitos de privacidade, as ameaças e controlos. Extraído de (Oetzel e Spiekermann, 2014).

Por fim, no **sexto e sétimo passo**, são avaliados os controlos sugeridos quanto à sua eficácia e viabilidade, e é produzido um documento final com o planeamento de implementação dos mesmos.

2.7.1 ICO (2014)

No Reino Unido, o *Information Comissioner's Office* (ICO) tem por missão defender os direitos à informação, a promoção da transparência dos órgãos públicos e a privacidade dos dados pessoais (ICO, sem data). A ICO é uma entidade independente reguladora, que controla a implementação da regulamentação relativa à proteção dos dados pessoais.

A ICO foi a primeira organização da Europa a publicar um guia orientador sobre análise de impacto à privacidade em 2007, tendo a última versão sido revista em 2014 (ICO, 2014).

Segundo a ICO, para que seja mais eficaz, o PIA deve ser incluído no início de vida dos projetos. Este processo é composto por 6 fases importantes:

1. Identificar a necessidade de um PIA;
2. Descrever os fluxos de informação;
3. Identificar os riscos relacionados com a privacidade;
4. Identificar e avaliar as ações para tratar os riscos;
5. Documentar as ações aprovadas;
6. Integrar os resultados no planeamento de projetos.

O primeiro passo do PIA é identificar a necessidade de avaliar os riscos da privacidade, questionando os objetivos do projeto e os benefícios do mesmo para a organização e para terceiras partes envolvidas, compreendendo quais as tipologias de

dados possivelmente envolvidas, as finalidades com que estas serão recolhidas e quais as tecnologias em que estas serão processadas e armazenadas. É importante que seja efetuado no início de vida do projeto, pois só assim se poderá avaliar os riscos envolvidos na implementação do mesmo.

Se for identificada a necessidade de efetuar um PIA, numa segunda fase devem ser documentados os fluxos de informação, descrevendo como a informação é recolhida, armazenada, processada e apagada. É importante que seja documentada de forma compreensiva toda a informação envolvida, caso contrário, poderão não ser identificados riscos para a privacidade numa fase posterior.

Na identificação dos riscos relacionados com a privacidade, a organização deve identificar potenciais problemas associados com a privacidade no desenvolvimento do projeto. São incluídos alguns exemplos de potenciais riscos para a privacidade, sendo que segundo a ICO estes podem ser categorizados quanto a sua conformidade legal, na organização e nos titulares. São, por exemplo, riscos de privacidade para os titulares, a recolha excessiva de dados pessoais, a informação recolhida ser usada para além do tempo de retenção definido e a alteração da finalidade da recolha sem o consentimento do seu titular. Já para a organização, são exemplos de riscos o impacto na reputação pela incerteza dos utilizadores relativamente à segurança com que a sua informação é armazenada, a exposição indevida de dados pessoais e as consequentes penalizações financeiras. Na conformidade cabem todos os riscos relacionados com o incumprimento de leis e legislação aplicável.

Na fase de identificação e avaliação das ações de tratamento, devem ser discutidas formas de tratar os riscos, por forma a eliminar, reduzir ou aceitar. Existem muitas formas de tratar os riscos de privacidade, como por exemplo, a decisão de recolher ou não os dados, assegurando que as pessoas envolvidas têm formação na proteção de dados, desenvolvendo formas de anonimização dos dados, informando de forma clara quais as finalidades da recolha dos dados, entre outros. Todas estas medidas, devem ser avaliadas quanto ao seu custo/beneficio para o desenvolvimento do projeto.

As medidas identificadas para tratar os riscos quer sejam para eliminar, reduzir ou aceitar devem ser documentadas, produzindo um relatório final que demonstra que o processo de avaliação foi efetuado de forma correta e que os riscos não aceites são controlados e tratados. A ICO encoraja ainda que o relatório final da avaliação seja publicado por uma questão de transparência para com a sua comunidade.

Por fim, os resultados devem ser integrados no planeamento do projeto, incluindo as medidas identificadas. Cada vez que o projeto tiver alterações, o PIA deve ser revisitado para garantir que este se mantem adequado.

2.7.2 AEPD (2014)

A Agência Espanhola para a Proteção de Dados (AEPD) apresentou em 2014, também uma metodologia para avaliação de risco na privacidade que vale a pena mencionar.

A abordagem apresentada pela AEPD, à semelhança da abordagem desenvolvida por Oetzel e Spiekermann (2014), inicia-se com uma reflexão da necessidade de ser efetuada uma análise de impacto aos dados pessoais, conforme se ilustra na Figura 7.

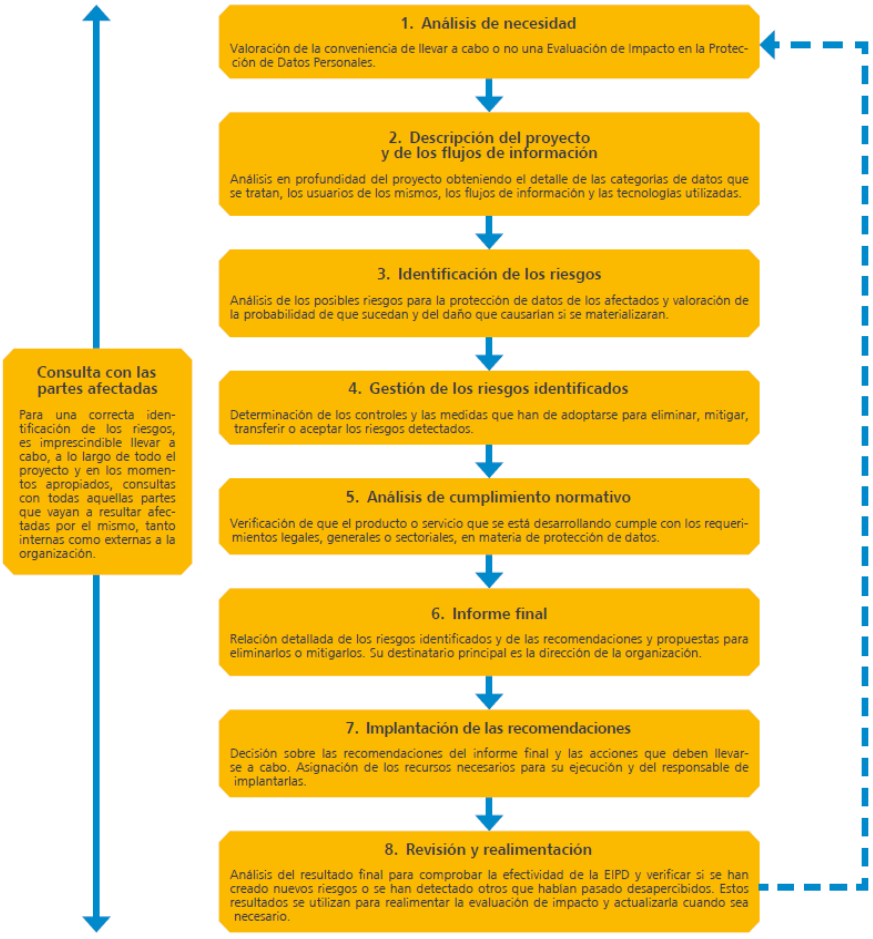

Figura 7 – Processo de avaliação de impacto na proteção dos dados. Extraído de (AEPD, 2014).

Sempre que sejam desenvolvidos novos projetos ou iniciativas, é fundamental levar a cabo uma reflexão da necessidade de efetuar uma avaliação de impacto. Nessa

reflexão vale a pena verificar se algumas situações em que se aconselha a execução de uma avaliação de impacto à proteção dos dados pessoais seja efetuada. No guia apresentado, são indicadas algumas situações em que deve considerar a avaliação de risco aos dados pessoais, nomeadamente:

- Quando se enriquece a informação recolhida sobre as pessoas, mediante a utilização de nova informação obtida a partir de outras fontes, ou quando se utiliza a informação recolhida para novas finalidades;
- Quando se efetue o tratamento deliberado de dados pessoais de pessoas menores de idade;
- Quando são efetuados tratamentos de modo a avaliar aspetos pessoais e a enquadrar em perfis que levam à determinação do seu comportamento e a tomada de decisões com efeitos jurídicos que afetam significativamente os titulares, especialmente quando provocam decisões discriminatórias;
- Quando existir o tratamento de um grande volume de dados pessoais através de tecnologias como o "*Big Data*", "*Internet of Things*" ou em "*Smart Cities*".

Após a identificação da necessidade de avaliação de impacto nos dados pessoais, e se verificar a existência de alguma das situações referidas que implicam a execução de um PIA, é desenvolvida a descrição do projeto, incluindo um resumo do mesmo, a sua necessidade e as oportunidades para a organização, identificação dos aspetos relevantes suscetíveis de criar mais riscos para a privacidade, os meios de tratamento utilizados e ainda as categorias de dados pessoais utilizadas e a justificação da sua necessidade.

Finda a descrição do projeto, é iniciada a avaliação do impacto do projeto analisando toda a documentação produzida até ao momento, em particular, o ciclo de vida dos dados pessoais envolvidos, as suas utilizações e finalidades assim como os utilizadores com acesso aos mesmos. Com esta primeira avaliação são identificados os riscos.

No guia apresentado pela AEPD, está incluída uma biblioteca de riscos que podem ser utilizados como referência no momento da execução de um PIA. Estes riscos são, por exemplo, o carecimento de legitimidade para o tratamento de dados pessoais, a impossibilidade de retirada de consentimento ao tratamento de dados pessoais por parte do seu titular, a finalidade da recolha dos dados pessoais não é transparente, entre outros.

Uma vez os riscos identificados, deve também considerado para a análise a existência de legislação em vigor nestas matérias que tenha impacto na implementação do projeto. A AEPD inclui como referência no seu guia algumas medidas para tratar os riscos identificados.

Por fim, é elaborado um relatório final, com recomendações e medidas a tomar para que o projeto cumpra com todos os requisitos impostos pela legislação em vigor nestas matérias.

Capítulo 3

O Contexto do DNS.PT

Neste capítulo é estudada a origem da Internet e do *Domain Name System* (DNS) e ainda a organização em estudo, o .PT. É ainda apresentado o processo de gestão de riscos do .PT nas vertentes da qualidade, segurança e continuidade de negócio do .PT e o sistema atualmente implementado na organização.

3.1 A Internet e o Domain Name System (DNS)

O conceito de "*Galactic Network*" desenvolvido em 1962 por Licklider e Clark, onde pela primeira vez se apresentava uma rede global de computadores, tornou-se no que hoje conhecemos por Internet. No conceito apresentado, pela primeira vez, qualquer pessoa podia através de um computador aceder a informação armazenada em qualquer um dos outros computadores integrantes desta rede.

A Internet nasceu nos anos 60, no seio de projetos de investigação financiados pelo governo dos Estados Unidos da América (EUA) motivada pelo ambiente geopolítico da Guerra Fria, com o objetivo de criar uma rede de comunicações resiliente à ameaça nuclear iminente da União Soviética (Almeida, 2005). Posteriormente a Internet passou a ser utilizada pelo meio académico, tendo sido nas redes académicas que foi massificado através da adoção e disseminação dos Protocolo de Controlo de Transmissão e do Protocolo de Internet (TCP/IP) nos computadores das Universidades, bem como através do desenvolvimento de aplicações inovadoras neste âmbito e passou a ser conhecido como Internet (Leiner *et al.*, 2009).

A Internet é uma rede de redes que interconecta milhares de dispositivos por todo o mundo através de meios de transmissão, como por exemplo fios de cobre, cabos coaxiais, fibras óticas e satélites, e através de meios de comutação, conhecimento por encaminhadores (*packet switches*). Cada um destes encaminhadores tem pelo menos

duas ligações: uma de entrada e uma de saída, que permite que os pacotes sejam comutados e trocados entre os dispositivos ligados a esta rede. A comunicação na Internet tem por base o protocolo IP. Este protocolo é responsável pelo endereçamento dos dispositivos, que é representado por um conjunto de octetos, e pelo encaminhamento dos pacotes.

Com o crescimento da Internet, tornou-se impraticável para os seus utilizadores a memorização da quantidade enorme de endereços IPs. Assim, com base no RFC 226, foi desenvolvido uma tabela chamada de "HOSTS.TXT", onde eram mapeados todos os endereços IPs e os respetivos *hostnames* pertencentes à rede (Karp, 1971). Este ficheiro era depois instalado e atualizado em todas as máquinas da rede, permitindo assim a utilização dos *hostnames* ao invés dos endereços IP. Esta abordagem, pecou pela sua pouca escalabilidade, difícil gestão e manutenção, e por isso também acabou por não ter sucesso. Foi assim que Paul Mockapetris em 1983, apresentou um sistema para ultrapassar o problema apresentado, o *Domain Name System* (DNS). Nos RFC 882 e RFC 883 (Mockapetris, 1983; P. Mockapetris, 1983), foi proposto um sistema com uma arquitetura distribuída e hierárquica que facilitava o uso da internet através da abstração dos endereços de IP em nomes de domínio. O DNS faz a tradução de nomes de domínio em endereços IP e endereços IP em nomes de domínio, e desta forma quando queremos aceder a página do .PT basta-nos escrever www.dns.pt ao invés de escrever o IP onde está alojado o serviço "185.39.208.69".

O DNS está organizado hierarquicamente, onde no topo estão os servidores-raiz, o ponto ".", conforme ilustrado na Figura 8. Nestes servidores são armazenados os endereços IPs de todos os *Top-Level Domain* (TLD). Existem dois grandes tipos de TLDs, entre eles estão os *Generic Top-Level Domain* (gTLD), onde se enquadram por exemplo o .COM e o .ORG, e os *Country Code Top-Level Domain* (ccTLD), onde cabe por exemplo o .PT e o .BR, e que são sempre caracterizados por duas letras.

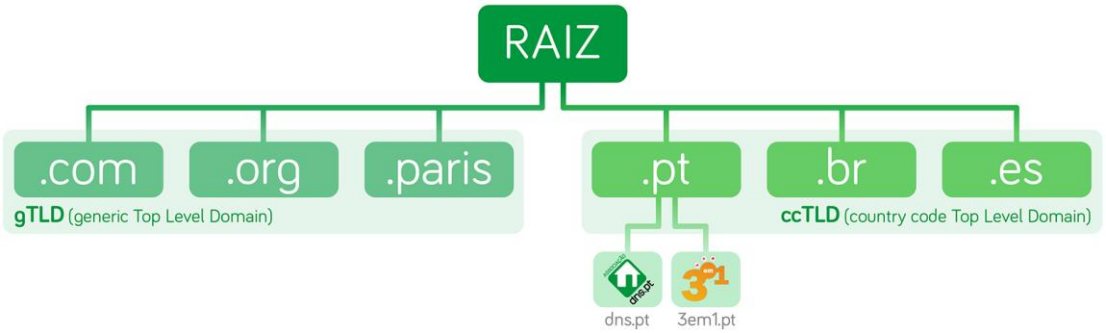

Figura 8 – Hierarquia do Domain Name System (DNS). Extraído de (DNS.PT, sem data).

Existem treze servidores-raiz distribuídos globalmente, geridos por doze organizações independentes, que são designados pelas letras A ao M (Root Server Technical Operations Association, sem data). Cada uma destas instâncias, são por sua vez replicadas de forma a garantir uma maior tolerância a faltas bem como um maior nível de performance do serviço.

Em Portugal, em 2004 foi configurada a primeira réplica dos servidores-raiz. Atualmente em Portugal existem cinco réplicas operacionais dos servidores L, F, J e E conforme ilustrado na Figura 9.

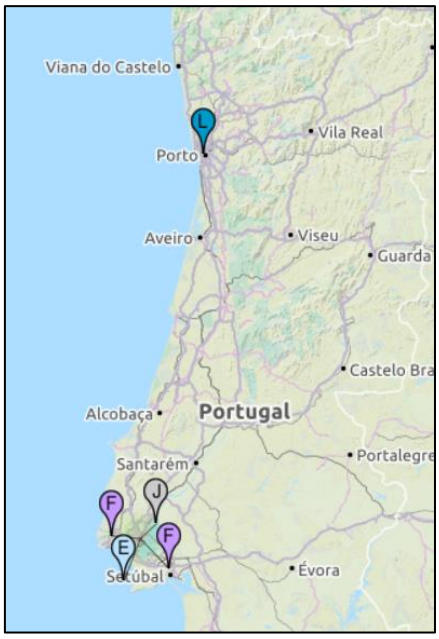

Figura 9 – Réplicas dos servidores-raiz no continente português. Adaptado de (Root Server Technical Operations Association, sem data).

3.2 A Associação DNS.PT

À semelhança do que sucedeu nos outros países, em Portugal o DNS foi introduzido por meio das redes de ensino e de investigação, onde o ccTLD de .PT foi operado e gerido pela Fundação para a Computação Científica Nacional (FCCN), desde a sua delegação a 30 de junho de 1988 até 2013.

Com a integração da FCCN na Fundação para a Ciência e a Tecnologia (FCT), nasce formalmente a Associação DNS.PT em 2013, com as competências de gestão, registo e manutenção do domínio de topo de Portugal .PT, delegadas pela *Internet Corporation for Assigned Names and Numbers* (ICANN, 2013).

A ICANN é uma organização multiparticipada, sem fins lucrativos e de âmbito internacional que por responsabilidade a distribuição de endereços IP, a designação de identificações de protocolo, a gestão do sistema de nomes de domínio de topo (TLD), com código genérico (gTLD) e de países (ccTLD) e ainda com funções de administração central da rede de servidores.

Todos os ccTLDs, independentemente da dimensão ou estrutura, têm por base as especificações inscritas no RFC1591 - "Estrutura do Sistema de Nomes de Domínio e a sua delegação" desenvolvido em 1994 (Postel, 1994). Os requisitos fundamentais à gestão, manutenção e operação de um TLD, são os deveres de, servir a comunidade, de estabelecer uma estrutura e capacidades organizacionais e técnicas para a realização das responsabilidades necessárias na prossecução de um trabalho equitativo, justo, honesto e competente, e por último de ser devidamente legitimado para a gestão do ccTLD por terem sido devidamente delegadas as funções e amplamente reconhecidas pela comunidade da Internet local.

O .PT é uma associação privada sem fins lucrativos que tem como fundadores a Fundação para a Ciência e a Tecnologia (FCT), a Associação da Economia Digital (ACEPI), a Associação Portuguesa para a Defesa do Consumidor (DECO) e um representante da *Internet Assigned Numbers Authority* (IANA).

O .PT adota um modelo de gestão multiparticipado, conforme a estrutura ilustrada na Figura 10. Este modelo está em consonância com as práticas adotadas internacionalmente, pelo que foi possível observar pelos dados apurados no plano de atividades do .PT (2013-2016), onde de um universo de 38 ccTLDs, 71% destas entidades eram de natureza associativa e sem fins lucrativos (DNS.PT, 2013b).

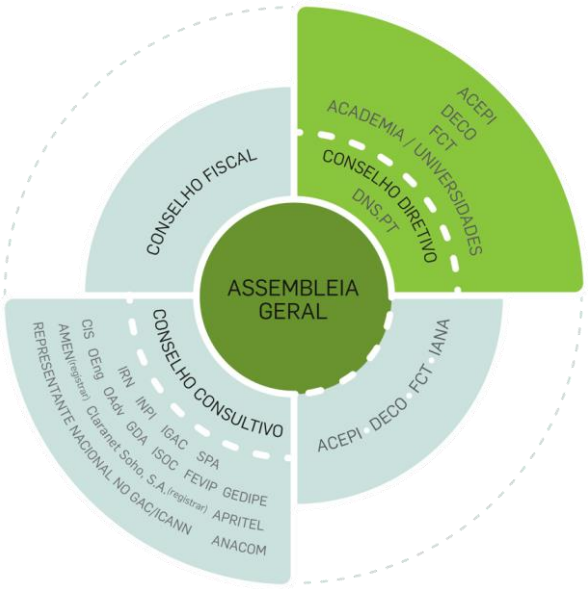

Figura 10 – Modelo de governação do .PT. Extraído de (DNS.PT, 2017a).

Atenta aos desenvolvimentos internacionais, o .PT acompanha de perto as evoluções dos sistemas e dos modelos de gestão dos seus pares, sendo relevante referir os seguintes marcos por este atingidos:

- Desde 2001, permite o registo através de Registrars;
- Desde 2003, permite a utilização de IPv6 nos servidores de nomes;
- Desde 2006, permite o registo de *Internationalised Domain Names* (IDNs);
- Desde 2007, o .PT é certificado na norma ISO 9001 – Sistema de Qualidade;
- Desde 2010, permite a assinatura de domínios com *Domain Name System Security Extensions* (DNSSEC);
- Desde 2012, o processo de registo de um domínio em .pt foi liberalizado;
- Desde 2015, o .PT é certificado na norma ISO/IEC 27001 – Sistema de Segurança da Informação;

Desde a adoção da norma ISO 9001, o .PT representa as atividades do negócio desenvolvidas através de diagramas. As suas atividades de negócio são agrupadas em macroprocessos, que podemos observar na Figura 11. Fazem parte dos macroprocessos, por exemplo, as atividades relativas ao registo e gestão de nomes de domínio .PT e de gestão de pessoas.

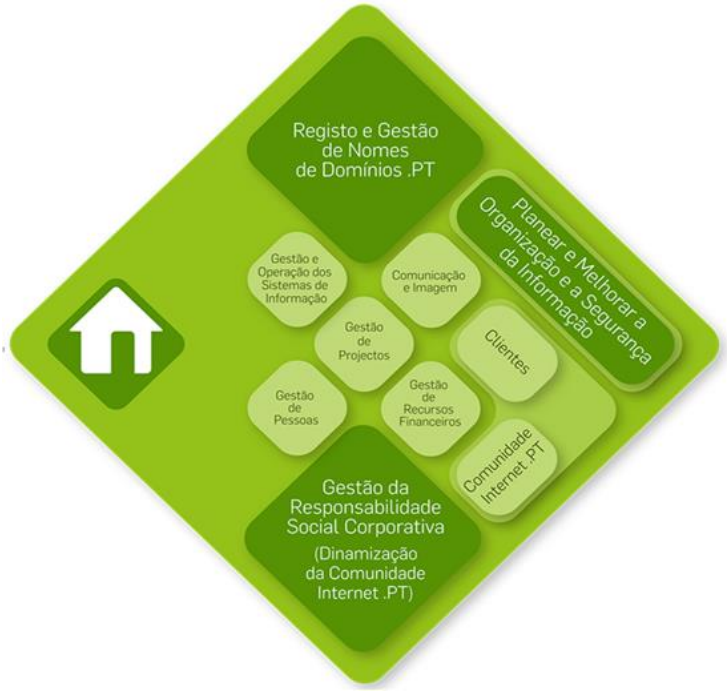

Figura 11 – Mapa de macroprocessos do .PT. Extraído de (DNS.PT, 2017a).

Os macroprocessos são constituídos por um conjunto de processos de negócio que descrevem funcionalmente as atividades do negócio da organização. É para cada um dos processos de negócio identificados os *inputs* e *outputs* esperados, os objetivos definidos e as partes interessadas.

Os objetivos pretendidos pelos processos de negócio são concretizados através de procedimentos. Cada processo de negócio pode ter um ou mais procedimentos associados. Os procedimentos são representados seguindo a linguagem *Business Process Model and Notation* (BPMN).

3.3 Gestão do risco no .PT

O .PT desenvolveu uma solução para gestão do risco, apoiado numa abordagem metodológica que foi sendo aperfeiçoada ao longo do tempo em função da maturidade do .PT para com as matérias da Qualidade e da Segurança da Informação. Esta plataforma foi desenvolvida sobre a tecnologia Microsoft Access, e permite efetuar todo o processo gestão do risco para a segurança da informação, qualidade e continuidade de negócio, que se encontra definido no sistema de Gestão de Qualidade e Segurança do DNS.PT. O procedimento de gestão de risco da organização encontra-se ilustrado na Figura 12, e permite efetuar as seguintes fases:

1. Comunicação;
2. Apreciação de Risco;
3. Tratamento de Risco;
4. Monitorização.

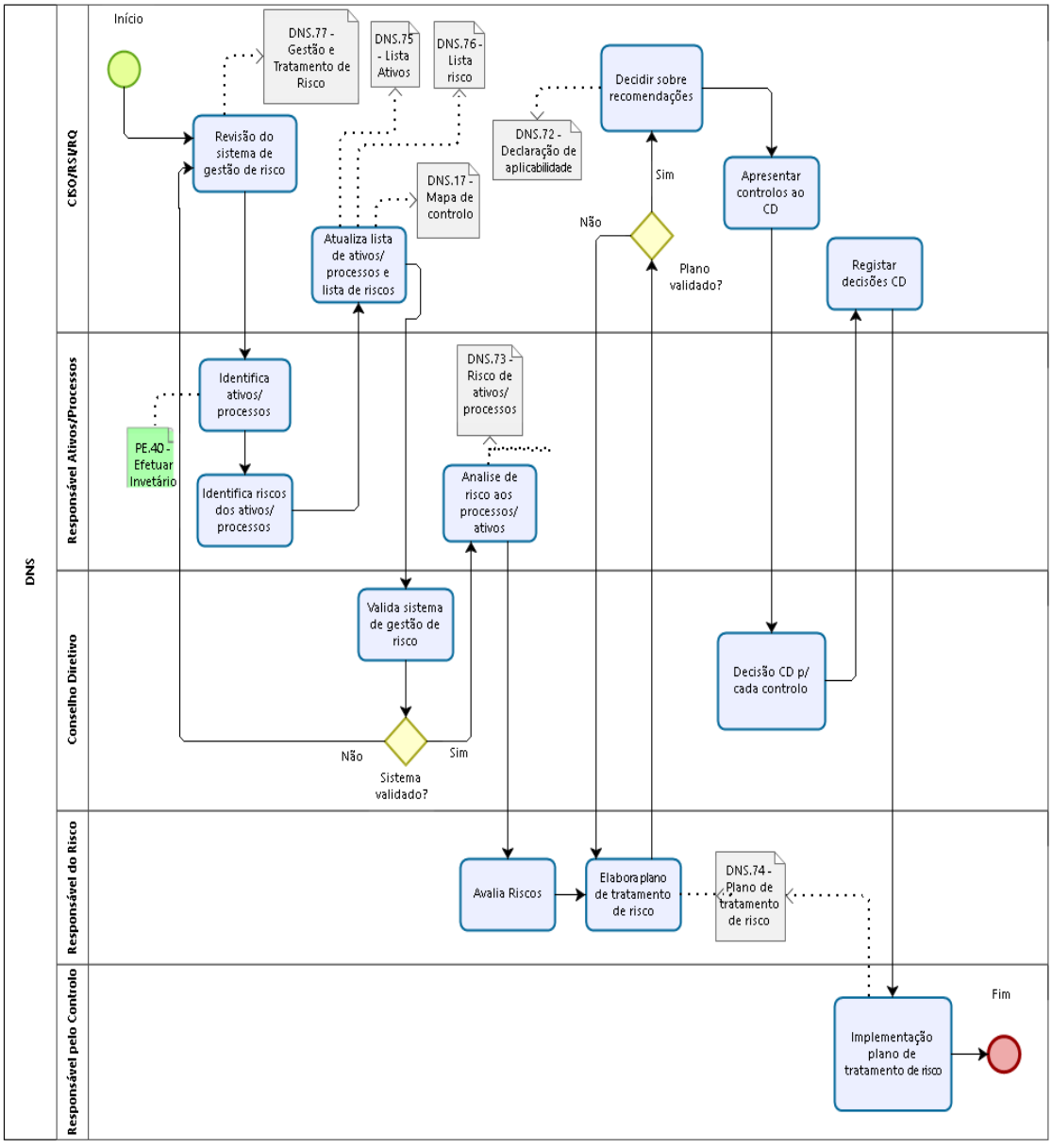

Figura 12 – Procedimento de negócio do .PT – Gerir e tratar o risco (PE.03).

A metodologia de gestão de risco implementada teve por base a ISO/IEC 27005:2011, sendo posteriormente adaptada para também enquadrar a continuidade de negócio e a qualidade e encontrando-se alinhada com as boas práticas do sector, com a legislação aplicável e com referenciais ISO/IEC 27001:2013 e ISO 9001:2015. A gestão

do risco no .PT tem por objeto, a identificação e tratamento de riscos nos seguintes domínios:

- **Segurança da Informação**: riscos que coloquem em causa a confidencialidade, integridade e disponibilidade dos ativos do .PT;
- **Continuidade de Negócio**: riscos que coloquem em causa o bom funcionamento dos processos de negócio críticos;
- **Qualidade**: riscos que coloquem em causa a disponibilização de um produto e/ou serviço conforme ou que afete a satisfação de clientes e parceiros.

O processo de gestão de risco inicia-se com a Comunicação**.** Nesta é efetuada a revisão integral do SGQSI, com a revisão de toda a documentação associada como as políticas de qualidade e segurança da informação, processos e procedimentos de negócio, de manuais auxiliares e do inventário dos ativos e posteriormente comunicadas quaisquer alterações relevantes às partes interessadas, colaboradores e fornecedores. Nesta fase todas as alterações são transpostas para o SGQSI, onde se podem registar os ativos, os riscos e os processos na plataforma de gestão de risco do .PT.

O segundo passo, a Apreciação de Risco, inicia-se com identificação, depois com a análise e por fim com a avaliação dos riscos. Inicialmente são identificados todos os riscos nos três âmbitos distintos Qualidade, Segurança da Informação e Continuidade de Negócio. Nesta fase é importante que todos os riscos sejam identificados, pois apenas estes riscos vão fazer parte da avaliação e poderão ser mitigados no seguimento deste processo. Os riscos identificados são registados na plataforma de gestão de risco do .PT, da qual se apresenta um ecrã na Figura 13. Aos riscos identificados são também associados os controlos que já estão implementados.

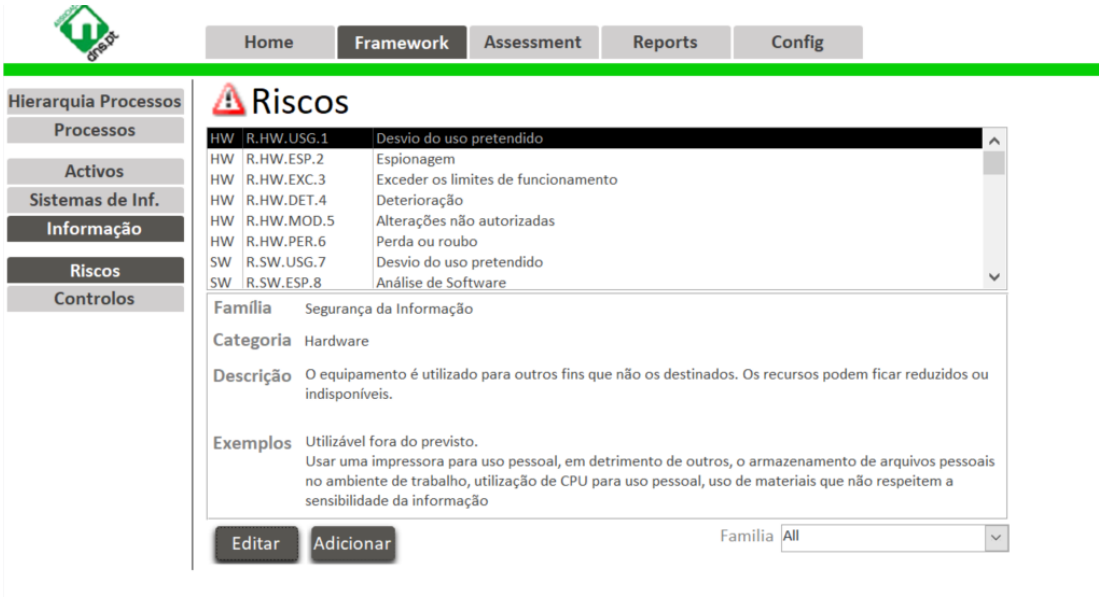

Figura 13 - Plataforma de gestão de risco do .PT – Menu biblioteca dos riscos.

Na fase da identificação dos riscos, para cada ativo é efetuada uma reflexão sobre quais os potenciais riscos que possam ter impacto no ativo em causa, e a verosimilhança com que cada um deles pode ocorrer. Esta identificação e avaliação é efetuada tendo por base uma escala quantitativa bem definida, tanto para o impacto (Tabela 2) como para a verosimilhança (Tabela 3), onde na verosimilhança o valor 1 corresponde a improvável e o valor 5 a bastante provável, e no impacto o valor 1 corresponde à classificação muito baixa e o valor 5 a muito alta.

Tabela 2 – Classificação do impacto. Extraído de (DNS.PT, 2017b).

Impacto	Confidencialidade	Integridade	Disponibilidade
1 – Muito Baixa	Poucos dados, dados públicos expostos.	Poucos dados, dados não críticos corrompidos.	Perda de serviço ligeira em componente secundário.
2 - Baixa	Muitos dados, dados públicos expostos.	Muitos dados, dados não críticos corrompidos.	Perda de serviço ligeira em componente primário.
3 - Moderada	Poucos dados, dados restritos expostos.	Poucos dados, dados críticos corrompidos.	Perda de serviço extensa em serviço secundário.
4 - Alta	Muitos dados, dados restritos expostos.	Muitos dados, dados críticos corrompidos.	Perda de serviço extensa em serviço primária.
5 – Muito Alta	Todos os dados expostos.	Todos os dados estão corrompidos.	Serviço completamente perdido.

Tabela 3 – Classificação da verosimilhança. Extraído de (DNS.PT, 2017b).

Verosimilhança	Classificação	Número de Ocorrências (O) por Ano
1	Improvável	O < 2
2	Pouco Provável	O >= 2 e O < 3
3	Provável	O >= 3 e O < 6
4	Bastante Provável	O >=6 e O <12
5	Muito Provável	O >= 12

O risco é calculado através do produto da verosimilhança e do impacto de um certo evento ocorrer. O impacto apurado corresponde à maior das vertentes analisadas, isto é, no caso da segurança da informação, para um dado evento o risco corresponde ao produto do maior impacto apurado nas vertentes confidencialidade, integridade e disponibilidade pela respetiva verosimilhança, conforme representado na Figura 14.

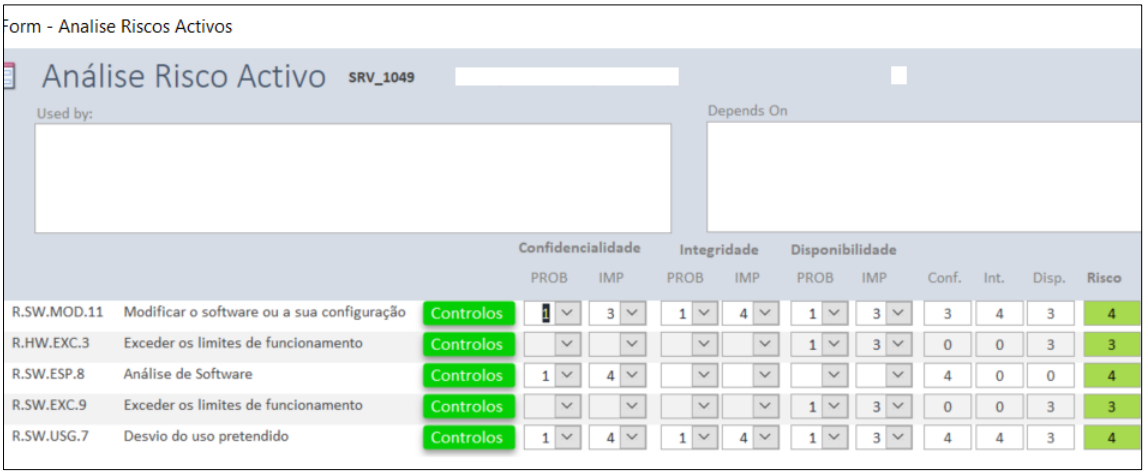

Figura 14 - Plataforma de gestão de Risco do .PT - Avaliação de riscos.

No caso da qualidade, o impacto é avaliado nas componentes da disponibilização de produto e/ou serviço conforme e na satisfação dos clientes e parceiros, e na continuidade de negócio nas componentes financeiras, reputação e na segurança e saúde dos colaboradores.

Por motivos de simplicidade no processo de avaliação do risco no .PT, os donos de cada um dos riscos avalia-os tendo em consideração os controlos implementados.

Sempre que um ativo tenha um risco superior ao aceitável pela organização, este carece de necessidade de ser tratado. Todos os riscos acima do aceitável são incluídos num plano de tratamento de risco, onde os responsáveis pelos ativos propõem novos controlos ou atualizações aos controlos existentes para tratar os riscos identificados. No

contexto do .PT, o risco não é aceitável sempre que é superior a 4, conforme se ilustra na tabela do cálculo do risco na Tabela 4.

Tabela 4 – Matriz de cálculo do valor de risco. Adaptado de (DNS.PT, 2017b).

Verosimilhança / Impacto	Muito Baixo (1)	Baixo (2)	Moderado (3)	Grave (4)	Muito Grave (5)
Bastante Provável (5)	5	10	15	20	25
Provável (4)	4	8	12	16	20
Pouco Provável (3)	3	6	9	12	15
Improvável (2)	2	4	6	8	10
Raro (1)	1	2	3	4	5

A cada controlo proposto para tratar os riscos são identificados os custos associados para que sejam avaliados os custos/benefícios da sua implementação, assim como a data prevista de implementação e o responsável pela implementação do mesmo. Na plataforma podemos gerir as ações do plano de tratamento de risco, através do menu exposto na Figura 15. Neste menu, é necessário registar a causa e a consequência do risco identificado, as ações de desenvolver para o tratar, o custo e o prazo estimado das ações a desenvolver e o risco residual estimado após implementação das ações. É ainda neste menu que se assinala que as ações já se encontram implementadas.

Figura 15 - Plataforma de gestão de risco do .PT – Tratamento de riscos.

Após o plano de tratamento do risco ter sido efetuado, este deve ser revisto com os donos dos ativos para elaborar uma proposta final para apresentar à gestão de topo.

As ações propostas após serem aprovadas são seguidas e registadas através do SGQSI. Na plataforma de gestão do risco do .PT é possível extrair relatórios das análises de risco e dos planos de tratamento associados, assim como listagens dos ativos, riscos e controlos.

Capítulo 4

Gestão do risco em segurança da informação e privacidade no .PT

Neste capítulo é descrito o modelo conceptualizado para a gestão dos riscos em segurança da informação e privacidade no contexto do .PT com base nas práticas estudadas anteriormente e ainda tendo em consideração o contexto da organização. É ainda desenhado o processo para aplicar o modelo desenvolvido e explicado detalhadamente cada um dos seus passos.

4.1 Modelo para gestão do risco em segurança da informação e privacidade

O risco para a privacidade surge quando existe um evento provável de colocar em causa o cumprimento dos requisitos impostos ao tratamento de dados pessoais. Estes requisitos nascem dos direitos consagrados no RGPD que se expõem na Tabela 1.

Assim, para cada um dos requisitos expostos na Tabela 1, podem surgir riscos que colocam em causa a segurança da informação e a privacidade dos dados no decorrer de uma operação ou um conjunto de operações sobre os dados pessoais, em particular as identificadas no n.º 2 do art.º 4.º do RGPD.

No contexto do .PT considera-se que existem três tipos de operações de tratamento de dados pessoais: a recolha, o armazenamento e o processamento. Consideram-se como processamento as atividades de organização, adaptação, consulta, comunicação e ainda transmissão de informação. As operações de tratamento de dados podem ser consideradas automatizadas, quando não requerem qualquer intervenção humana. O incumprimento dos diferentes requisitos no tratamento de um determinado ativo resulta num risco para a privacidade.

Considera-se no .PT que para a boa prestação do serviço, em conformidade com as boas práticas de segurança da informação e com as obrigações legais, o cumprimento destes requisitos é um requisito para o negócio. Considera-se ainda que além dos requisitos elencados no RGPD, são também relevantes os requisitos de segurança da informação, nomeadamente, os dispostos na norma ISO/IEC 27001 para proteger a informação pessoal.

Atendendo ao facto de que no .PT todos os processos de negócio estão documentados e representados através dos procedimentos que os compõem, o modelo foi desenvolvido com base nesta realidade. Assim, para cada processo de negócio do .PT são conhecidos os requisitos que a estes se aplicam, designadamente, a necessidade do direito à informação ou ainda da aplicação de controlos criptográficos mais rigorosos. São ainda conhecidos os ativos de informação envolvidos e respetivas operações de tratamento.

Para cada risco identificado podemos associar um ou mais controlos. A Figura 16 representa o modelo proposto.

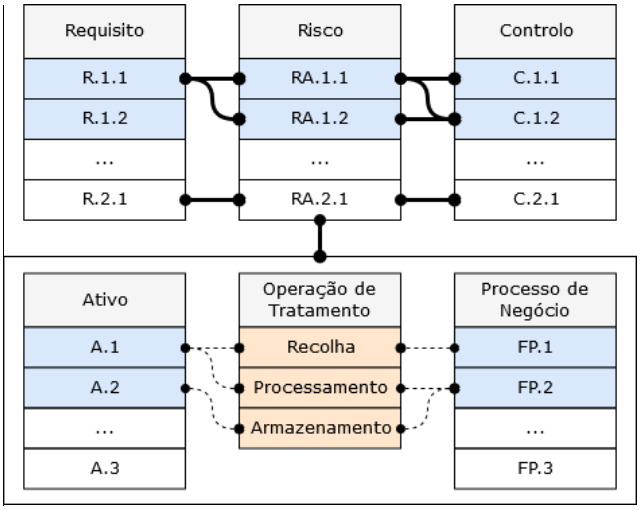

Figura 16 – Modelo proposto para a gestão de risco na privacidade no .PT.

Os ativos estão organizados hierarquicamente, conforme ilustrado na Figura 17, e podem ser do tipo: serviço, aplicação, servidor, localização e informação.

O ativo de informação pode existir em dois formatos, o lógico e o físico. Por informação em formato lógico entende-se que seja, por exemplo, faturas com dados de clientes em papel, e em formato lógico, dados dos clientes recolhidos através da plataforma online de registo do .PT. Qualquer informação é considerada pessoal quando

corresponde à definição de dado pessoal do art.º 4.º do RGPD, independentemente do seu formato.

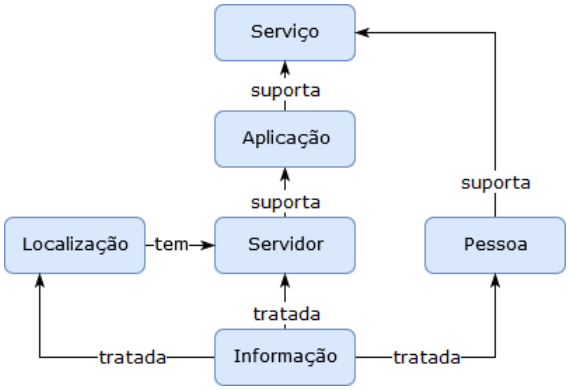

Figura 17 – Estrutura de ativos do modelo de gestão do risco proposto.

As operações de tratamento de informação são suportadas por um servidor quando em formato lógico ou por uma localização quando em formato físico. Entende-se por localização um espaço físico como por exemplo o Escritório do .PT. As operações de tratamento quando não automatizadas requerem a intervenção manual de um colaborador do .PT.

Os serviços oferecidos são suportados por uma aplicação ou conjunto de aplicações que são por seu turno suportadas nos servidores. Os servidores suportam as aplicações numa dada localização. Por serviço entendemos por exemplo, o conjunto de aplicações que permitem a receção e o envio de e-mails.

O modelo proposto é aplicado no contexto da organização em estudo, o .PT, dando suporte ao processo de gestão do risco da privacidade.

4.2 Processo para gestão do risco em segurança da informação e privacidade

Considerando os requisitos impostos pelo RGPD, o atual processo de gestão de risco em vigor no .PT (Figura 12) e ainda as boas práticas da ISO 31000:2009 (ISO, 2013) e dos casos estudados anteriormente, propõe-se o processo ilustrado na Figura 18, para a gestão dos riscos que colocam em causa a privacidade.

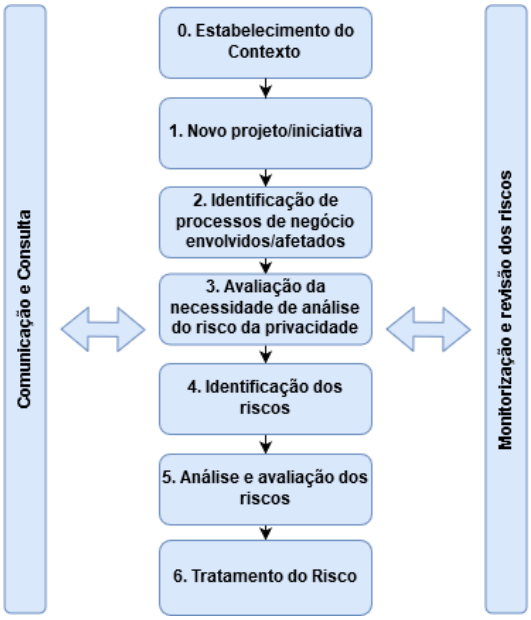

Figura 18 – Processo proposto para gestão do risco.

O processo de gestão de risco proposto, à semelhança do que se observa na ISO 31000:2009 (ISO, 2013), é composto por sete passos onde é estabelecido o contexto para a gestão do risco, onde são identificados novos projetos/iniciativas e os ativos associados, onde são avaliados os riscos para a privacidade e por fim, desenvolvido um plano de tratamento para os mesmos. Fazem ainda parte do processo de gestão de risco, duas etapas transversais, que podem ser desencadeadas em qualquer momento do processo, a comunicação e consulta das partes interessadas e a monitorização e revisão dos riscos.

No que respeita à etapa transversal da **Comunicação e Consulta**, cada uma das partes interessadas identifica os objetivos dos projetos/iniciativas, a informação pessoal objeto de tratamento, a finalidade do seu tratamento e os potenciais riscos associados ao mesmo. Na etapa de **Monitorização e Revisão dos Riscos** é levada a cabo a revisão regular dos controlos, para garantir que se mantêm eficazes na proteção dos dados pessoais, são identificados riscos emergentes, é avaliada a necessidade de rever as análises de risco efetuados. Na monitorização dos riscos é importante conseguir consultar os riscos com nível superior ao aceitável.

Passo 0 – Estabelecimento do Contexto

O .PT conta com um SGQSI, onde estão definidas as atividades desenvolvidas pelo .PT, ilustrado na Figura 11, cada uma destas atividades tem um objetivo

identificado, entradas e saídas esperadas. As partes interessadas têm expectativas quanto ao cumprimento do objetivo esperado. Por exemplo, na atividade de registo e gestão de nomes de domínio, os clientes, que são uma parte interessada, esperam que o seu domínio seja registado corretamente, esperam receber num prazo aceitável resposta aos seus pedidos de esclarecimentos e ainda que a sua informação pessoal seja disponibilizada no sistema Whois se assim o solicitarem.

O processo de gestão de risco para a privacidade proposto tem em consideração a metodologia atualmente em vigor no .PT (DNS.PT, 2017b), e tem por objetivo de forma sistemática, sempre que surgem novas atividades no .PT ou alterações relevantes às mesmas, considerar os riscos associados a estas atividades tendo em conta os princípios de privacidade e de segurança da informação, facilitando desta forma, logo desde a sua conceção a introdução das boas práticas no tratamento de informação pessoal.

São considerados riscos todos os eventos que possam colocar em causa a privacidade dos dados. O valor do risco é encontrado através do produto dos valores da verosimilhança e do impacto. Sempre que sejam identificados diferentes riscos para um mesmo ativo, o risco é o maior dos produtos encontrados. Para avaliar a verosimilhança dos riscos é utilizada a escala representada na Tabela 3 e para quantificar o impacto é utilizada a Tabela 5.

Tabela 5 – Tabela de impacto na privacidade em linha com metodologia de risco do .PT

Impacto	**Privacidade**
Muito Baixo (1)	Comprometimento de algum dos direitos dos titulares dos dados não suscetível de implicar um risco para os seus direitos e liberdades e/ou causar danos à organização.
Baixo (2)	Comprometimento de algum dos direitos dos titulares dos dados pouco suscetível de implicar um risco para os seus direitos e liberdades e/ou causar danos à organização.
Moderado (3)	Violação de algum dos direitos dos titulares dos dados suscetível de implicar um risco moderado para os seus direitos e liberdades e/ou causar danos à organização. Obrigatoriedade de comunicar o incidente à autoridade de controlo.
Alto (4)	Violação de algum dos direitos dos titulares dos dados suscetível de implicar um elevado risco para os seus direitos e liberdades e/ou causar danos à organização. Obrigatoriedade de comunicar o incidente à autoridade de controlo e ao titular dos dados.
Muito Alto (5)	Violação de algum dos direitos dos titulares dos dados suscetível de implicar um risco muito elevado para os seus direitos e liberdades e/ou causar danos à organização. Obrigatoriedade de comunicar o incidente à autoridade de controlo e ao titular dos dados.

O nível de risco aceitável para a organização é o mesmo que atualmente está em vigor, ou seja, um risco é aceitável quando o cálculo do produto dos valores da verosimilhança pelo impacto tem um resultado inferior a cinco.

Passo 1 – Novo projeto/iniciativa

Para cada novo projeto/iniciativa ou alteração relevante nos processos de negócio do .PT, é então despoletado o processo de identificação dos processos de negócio e dos ativos associados e respetivas operações de tratamento.

Passo 2 – Identificação de processos de negócio e ativos de informação

No desenvolvimento ou alteração relevante de um projeto/iniciativa são identificados, pelo responsável pelo projeto/iniciativa, os processos de negócio afetados, os ativos que lhe dão suporte e a informação pessoal que é irá ser objeto de tratamento. No processo de identificação dos ativos, devem ser incluídos, conforme disposto nos artigos 13.º, 14.º e 15.º do RGPD, os ativos que:

- Recolhem informações pessoais, tendo em conta a sua localização geográfica;
- Armazenam informações pessoais, tendo em conta a sua localização geográfica;
- Processam informações pessoais, tendo em conta a sua localização geográfica.

Para cada um dos ativos, é identificada a informação objeto de tratamento. Cada ativo de informação, sempre que possível, deve incluir na sua enumeração:

- A finalidade do tratamento dos dados pessoais, como por exemplo, gestão de clientes, medicina no trabalho ou ainda para efeitos de seguros de saúde;
- A legitimidade do tratamento, de acordo com as condições de licitude enumeradas no art.º 6.º do RGPD;
- Os prazos conservação da informação definidos atualmente na organização;
- O dono do ativo, isto é, a pessoa ou departamento com a função de assegurar que todas as medidas de tratamento de risco identificadas são implementadas.

Passo 3 – Avaliação da necessidade de análise do risco da privacidade

De acordo com os requisitos dispostos no art.º 35.º do RGPD e do projeto de regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (CNPD, 2018), é verificada a

necessidade de proceder à apreciação dos riscos da privacidade através da identificação, análise e avaliação dos riscos. Esta necessidade verifica-se quando as operações de tratamento realizadas sobre os dados pessoais possam representar "um elevado risco para os direitos e liberdades das pessoas singulares" pelo n.º 1 do art.º 35.º do RGPD. Considera-se elevado risco quando algum dos tratamentos efetuados corresponde a alguma das situações enumeradas na Tabela 6. Esta fase é também realizada pelo responsável do projeto/iniciativa e quem este considerar relevante incluir nesta fase.

Tabela 6 – Tabela de avaliação de necessidade de análise de risco na privacidade de acordo o art.º 35.º do RGPD e projeto de regulamento n.º 1/2018.

Requisitos	**Sim/Não**
(art.º 35.º, n.º 1) Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais; Ex.: A utilização da impressão digital ou de reconhecimento facial para melhorar o controlo do acesso físico;	
(art.º 35.º, nº 3) Avaliação sistemática e completa de aspetos pessoais, como por exemplo a definição de perfis ou a monitorização de zonas acessíveis ao público em grande escala. Ex.: Videovigilância à entrada do edifício do local de trabalho.	
(art.º 9.º e 10.º) Tratamento de dados sensíveis ou de natureza altamente pessoal. Ex.: Dados de saúde geridos por uma clínica ou hospital.	
(art.º 35.º, n.º 3) Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente o titular dos dados.	
(considerando 75) Tratamento de dados relativos a titulares de dados vulneráveis. Ex.: Os titulares de dados vulneráveis podem incluir por exemplo crianças e idosos.	
(art.º 22.º) Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato. Ex.: Uma empresa de comércio eletrónico só proceda ao envio/entrega do bem caso o cliente e titular dos dados consinta na transferência dos seus dados pessoais para uma empresa de marketing direto.	

Passo 4 – Identificação dos riscos

Nesta fase, são identificados os riscos que podem colocar em causa a proteção dos dados pessoais pelo dono do ativo. Para cada um dos ativos de informação em análise, o dono do ativo identificada os riscos tendo em atenção as operações de tratamento a que este é sujeito, isto é, onde e como é recolhido, processado e armazenado, e ainda a finalidade e legitimidade do tratamento. Podem existir dois tipos distintos de riscos: aqueles que colocam em causa o exercício dos direitos dos titulares dos dados, como por exemplo, o direito à informação e à portabilidade dos dados, e os riscos que

colocam em causa a segurança da informação pessoal, como é o roubo ou ainda a alteração não autorizada de informação pessoal.

Os riscos que colocam em causa exercício dos direitos dos titulares dos dados, relevantes no contexto do .PT, são enumerados na Tabela 7.

Tabela 7 – Exemplos de riscos identificados para a privacidade no âmbito do .PT

Risco	**Requisito**	**Dono**
Recolha excessiva de dados pessoais	Direito à limitação da finalidade	DGA
Proteção de dados comprometida em transferências internacionais	Direito à informação Direito à oposição Direito à limitação da finalidade	DGA
Incumprimento do dever de informação	Direito à informação	DGA
Impossibilidade de exercício do direito de acesso	Direito ao acesso	DGA
Impossibilidade de exercício do direito ao esquecimento	Direito ao esquecimento	DGA
Incapacidade de resposta atempada aos pedidos dos titulares dos dados	Direito à informação	DGA
Falta de mecanismos ou políticas de eliminação de dados pessoais (períodos de retenção excessivos)	Direito à limitação da finalidade	DGA
Tratamento de dados excede a finalidade	Direito à limitação da finalidade	DGA
Consentimento inválido	Direito à informação Direito à oposição	DGA
Impossibilidade de exercício do direito de portabilidade de dados	Direito à portabilidade	DGA
Impossibilidade do exercício do direito de oposição	Direito à oposição	DGA
A qualidade dos dados pessoais é comprometida	Direito à retificação Direito à oposição	DGA

Os riscos que colocam em causa a segurança da informação pessoal, encontram-se enumerados na Tabela 8. Estes riscos decorrem do art.º 33.º do RGPD, onde é prevista a notificação obrigatória à autoridade de controlo, "sempre que exista uma violação de dados pessoais, sem demora injustificada e, sempre que possível, até o prazo máximo de 72 horas após ter tido conhecimento" (RGPD, 2016).

Tabela 8 – Exemplos de riscos de segurança da informação que podem colocar em causa a privacidade.

Risco	**Requisito**	**Dono**
Alteração não autorizada de informação	Notificação de violação de dados	DGA
Leitura não autorizada de informação	Notificação de violação de dados	DGA
Perda ou roubo de informação	Notificação de violação de dados	DGA
Escuta não autorizada de comunicações	Notificação de violação de dados	DGA
Alterações não autorizadas nas comunicações	Notificação de violação de dados	DGA
Erro humano no manuseio da informação	Notificação de violação de dados	DGA

Passo 5 – Análise e avaliação dos riscos

Para cada um dos ativos de informação pessoal identificados no âmbito de um processo de negócio em análise, são analisados e avaliados os riscos que podem colocar em causa a privacidade. A análise e avaliação dos riscos é efetuada pelo dono dos ativos. Os riscos identificados são avaliados quanto à sua verosimilhança de acordo com a Tabela 3 e quanto ao seu impacto de acordo com Tabela 5. Na avaliação do impacto é levado em consideração os controlos implementados. A ponderação do impacto pode assim ser reduzido pelos controlos existentes.

O risco resulta do produto dos fatores da verosimilhança e do impacto na privacidade. Sempre que um ativo tem mais que um risco identificado, considera-se o maior dos riscos identificados.

Passo 6 –Tratamento de risco

Após a avaliação dos riscos, sempre que sejam observados riscos cuja avaliação tenha valor de risco superior ao nível definido como aceitável pelo .PT, devem ser identificados pelos donos dos riscos controlos para os tratar por forma a eliminar, mitigar, transferir ou aceitar o risco. Cada controlo identificado deve indicar a causa raiz do risco, um plano de ações, a prioridade, data prevista para implementação e custo associado e ainda o risco residual estimado após implementação do mesmo.

O processo de gestão de risco da privacidade proposto é apresentado na secção 4.3 com a sua aplicação para um processo de negócio do .PT.

4.3 Gestão de risco em segurança da informação e privacidade no .PT

Aplicando o processo para a gestão do risco em segurança da informação e privacidade proposto, foi estabelecido o contexto da organização através da consideração das atividades desenvolvidas no .PT e as respetivas partes interessadas.

A atividade principal do .PT, isto é, o registo de nomes de domínio de .PT, foi utilizada como caso prático para demonstrar a sua aplicação no contexto da organização. A atividade de registo de nomes de domínio do .PT, está descrita num procedimento interno da organização. Foi a partir da representação do procedimento registo de nomes de domínio do .PT que foi possível identificar os ativos que o

suportavam e que serviram para testar o modelo desenvolvido de gestão de risco em segurança da informação e privacidade.

No procedimento de registo de nomes de domínio do .PT, em primeira instância, é verificado se o nome de domínio alvo de registo está disponível, isto é, não está já registado por outra entidade ou proibido para registo. Verificando-se que o domínio se encontra disponível para registo, é então possível submeter pela entidade titular o registo de domínio para ser validado pelo .PT. A equipa do .PT verifica o registo quanto ao seu cumprimento com os requisitos técnicos e financeiros. Quando se verificam os requisitos o domínio passa a estar ativo, ficando disponibilizado na zona do .PT, e a entidade titular é notificada do mesmo. É ainda neste procedimento, que o domínio passa por uma avaliação jurídica. Sempre que o nome de domínio não cumpra com as regras de nomes de domínios de .PT, este pode ser removido. Este procedimento enquadra-se no âmbito do processo de negócio registo de domínios (FP.20), que se encontra representado no macroprocesso na Figura 19, registo e gestão de nomes de domínios .PT (MP.07).

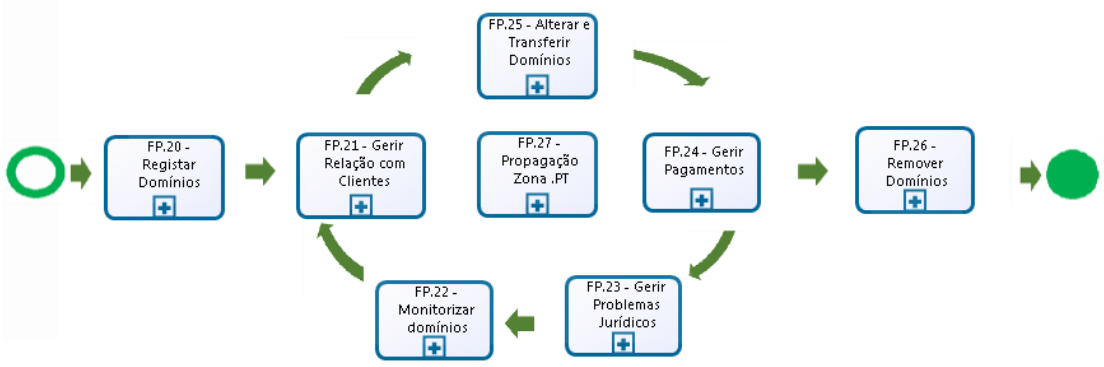

Figura 19 – Macroprocesso do .PT - Registo e gestão de nomes de domínios .PT (MP.07).

Foram identificados os ativos, com o apoio da equipa do .PT, em particular os ativos de informação pessoal tratados no âmbito desta atividade, do qual resultou a lista apresentada na Tabela 9.

Tabela 9 – Ativos de informação identificados para o procedimento - Registo de domínios .PT (PE.47)

Detalhe do Ativo	Recolha		Armazenamento		Processamento		Finalidade	Legitimidade	Conservação	Dono
	Geografia	Ativo	Geografia	Ativo	Geografia	Ativo				
Ficha de Contacto	PT	BD Front End	PT	BD Front End	PT	BD Front End	Gestão de Clientes	Relação Contratual	-	DGA
Nic-handle	PT	SIGA	PT	SIGA	PT	SIGA, WHOIS	Gestão de Clientes	Relação Contratual	-	DGA
Credenciais (nome, password)	PT	SIGA	PT	SIGA	PT	SIGA, WHOIS	Gestão de Clientes	Relação Contratual	-	DGA
IP e/ou Nameservers	PT	SIGA	PT	SIGA, WHOIS	PT	-	Gestão de Clientes	Relação Contratual	-	DGA
Email de criação de contacto	PT	SIGA	PT	SIGA, E-MAIL	PT	SIGA, E-MAIL	Gestão de Clientes	Relação Contratual	-	DGA
Nome do representante para pessoa coletiva	PT	SIGA	PT	SIGA	PT	-	Gestão de Clientes	Relação Contratual	-	DGA
Comprovativo de registo	PT	SAPERION	PT	SAPERION	PT	-	Gestão de Clientes	Relação Contratual	-	DGA

De seguida, para cada um destes ativos foram identificados os riscos que colocavam em causa a privacidade destes mesmos dados e avaliados quanto ao seu impacto e verosimilhança. Assim resultou, por exemplo, que os dados "Ficha de Contacto" no sistema Whois incorriam no risco de incumprir com o direito à informação com verosimilhança de 2 e impacto de 4 (Risco de 8), uma vez que, a informação acerca do tratamento dado a estes é prestada pelos parceiros do .PT e, portanto, fora do seu controlo. Uma vez que o risco identificado estava acima do risco aceitável (5) para a organização, foi sugerida a implementação de auditorias regulares efetuadas pelo .PT ao cumprimento do direito à informação por parte dos seus parceiros, e desta forma diminuir a verosimilhança deste risco.

Capítulo 5

Aplicação para gestão do risco em segurança da informação e privacidade no .PT

Neste capítulo é apresentada a arquitetura da aplicação desenvolvida no contexto do .PT para a gestão do risco em segurança da informação e privacidade, o seu modelo de dados e a tecnologia em que foi desenvolvida. É demonstrado o processo de gestão de risco na privacidade na aplicação desenvolvida. São apresentados os resultados dos testes realizados e as conclusões que resultaram do mesmo.

5.1 Arquitetura da aplicação

Com base no processo de gestão de risco desenhado no capítulo anterior, foi desenvolvido um sistema que permitisse a sua aplicação e teste no âmbito do .PT. O software foi desenvolvido na linguagem C# com base na *framework* ASP.NET Core[2] que utiliza o padrão de arquitetura de software Modelo-Visão-Controlador[3] (MVC). A arquitetura de desenvolvimento foi selecionada por se adaptar ao ambiente atualmente em produção no .PT, por ser um ambiente de desenvolvimento *opensource*, por permitir o fácil desenvolvimento de aplicações web e ainda por ser multiplataforma, isto é, permitir o seu desenvolvimento e publicação tanto em ambientes Windows como em ambientes Linux. Com base no padrão MVC, a aplicação foi desenvolvida em três camadas distintas, o Modelo, a Visão e o Controlador, como se pode observar na Figura 20. No padrão MVC, as camadas têm as seguintes funções:

[2] A framework está disponível no respositório https://github.com/aspnet/Home.
[3] Model-View-Controller na literatura anglo-saxónica.

- A camada do **Modelo** descreve toda a lógica do negócio, como por exemplo as operações de acesso aos dados. Neste padrão, a camada do Modelo recebe e responde a comandos através da camada Controlador.
- A camada da **Visão** gera a representação da informação a apresentar ao utilizador, isto é, a página a mostrar ao utilizador, e é responsável por responder aos pedidos do utilizador.
- A camada do **Controlador** é responsável por receber todos os pedidos do utilizador. O Controlador solicita a informação necessária à camada do Modelo que depois processa e envia a informação à Visão.

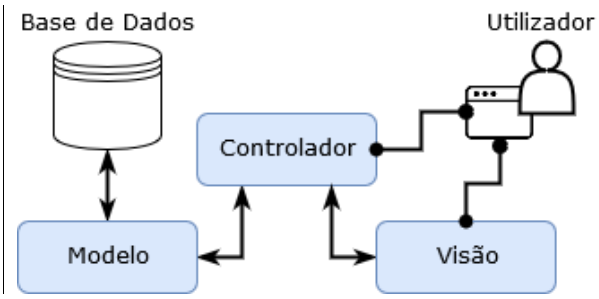

Figura 20 – Padrão de arquitetura de software adotado - MVC.

5.2 A aplicação

A aplicação foi desenvolvida no contexto do .PT em ambiente Windows, recorrendo à ferramenta disponibilizada pela Microsoft, o Visual Studio 2017[4] e utilizando o sistema de gestão de base de dados Microsoft SQL Server Express 2017[5]. O desenvolvimento iniciou-se com a definição e construção do modelo de dados, cujo diagrama é exposto na Figura 21.

[4] Disponível em https://visualstudio.microsoft.com/pt-br/vs/
[5] Disponível em https://www.microsoft.com/pt-pt/sql-server/sql-server-editions-express

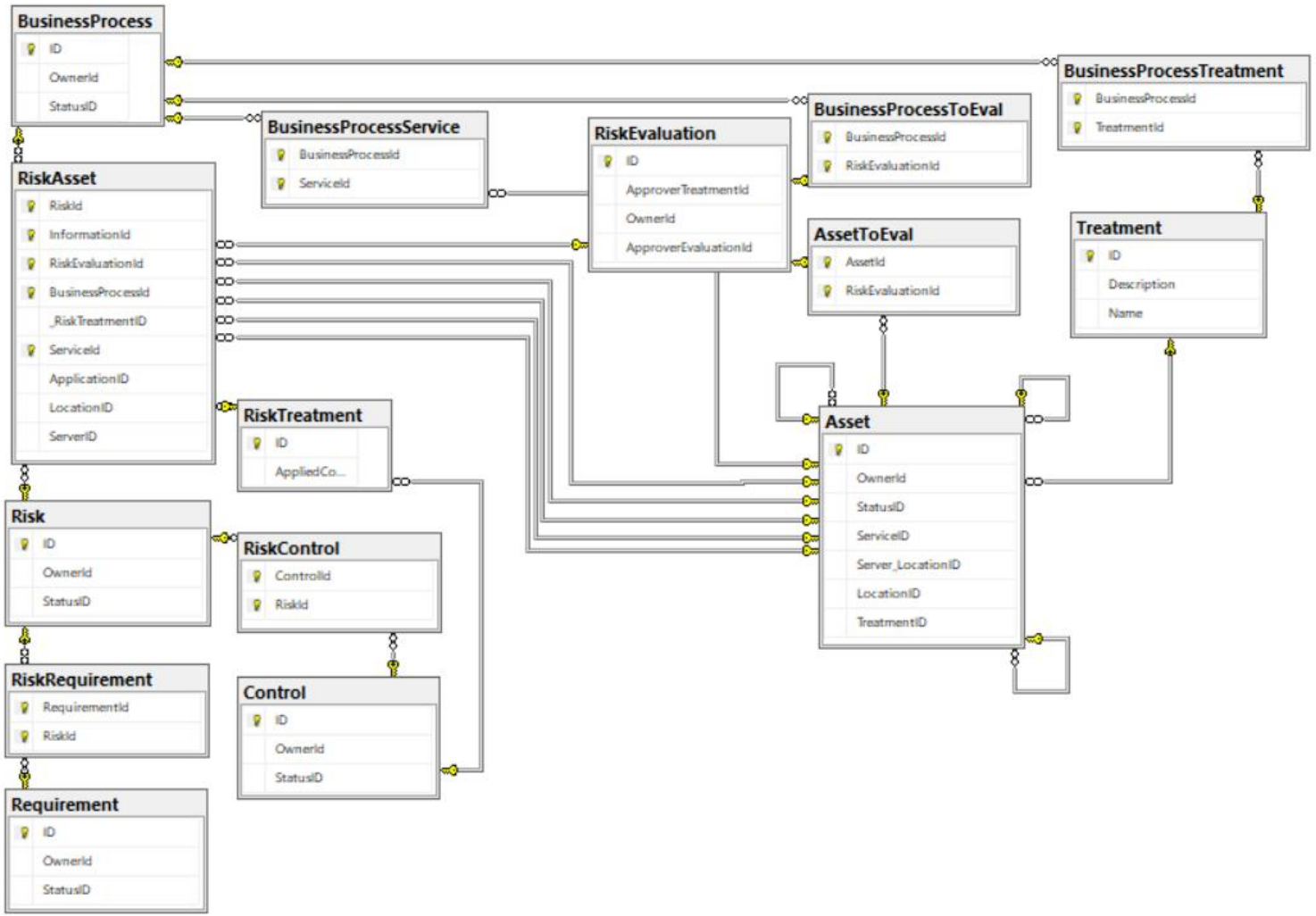

Figura 21 – Modelo relacional da base de dados da aplicação proposta.

O modelo de dados para a aplicação proposta é constituído pelas seguintes entidades:

- **Ativo (Asset):** Entidade que armazena todos os ativos e a informação associada a cada um destes. São por exemplo armazenados os serviços, com o seu nome e aplicações que suportam o mesmo.
- **Processo de Negócio (BusinessProcess):** Entidade que armazena todos os processos de negócio e a informação associada a cada um destes. É armazenado por exemplo o processo de negócio, com o seu nome e serviços que o suportam.
- **Risco (Risk):** Entidade que armazena todos os riscos e a informação associada a cada um destes. É armazenado por exemplo um risco, com o seu nome, o seu dono e a sua família.
- **Requisito (Requirement):** Entidade que armazena todos os requisitos e a informação associada a cada um destes. É armazenado por exemplo um requisito, com o seu nome, o seu dono, e a sua família.
- **Controlo (Control):** Entidade que armazena todos os controlos e a informação associada a cada um destes. É armazenado por exemplo um controlo, com o seu nome, o seu dono, e a sua família.
- **Tratamento (Treatment):** Entidade que armazena todos as operações de tratamento possíveis. É armazenado por exemplo uma operação de tratamento e a sua descrição.

As restantes tabelas que podemos observar no modelo servem para relacionar as entidades enumeradas acima. Por exemplo, a tabela “RiskControl” serve para associar a entidade Risco ao Controlo.

Importa referir que, quando é iniciada uma apreciação do risco, é criada uma nova instância armazenada na tabela “RiskEvaluation”. É nesta instância que são identificados os ativos a avaliar. Cada risco identificado num ativo e as respetivas ponderações efetuadas são armazenada na tabela “RiskAsset”. Em relação ao tratamento do risco, os controlos identificados, o plano de ações e os prazos previstos para implementação são armazenados na tabela “RiskTreatment”.

A aplicação desenvolvida conta com dois menus na página principal, o “Library” e o “Risk Management”. No primeiro menu, “Library”, como podemos observar na Figura 22, é possível aceder à biblioteca dos ativos, processos de negócio, requisitos, riscos e controlos, e ainda para cada um destes, adicionar, editar e remover se necessário.

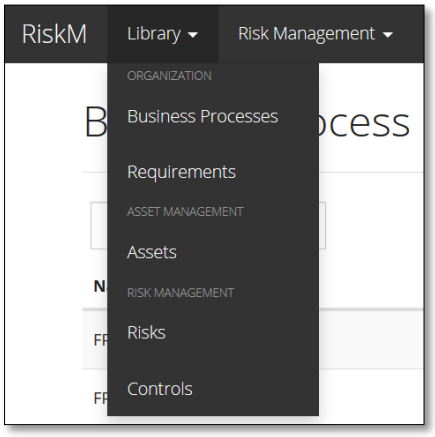

Figura 22 – Menu Biblioteca (“Library”) para gestão dos ativos, processos de negócio, requisitos, riscos e controlos.

Já no segundo menu, o “Risk Management”, conforme ilustrado na Figura 23, podemos despoletar uma análise de risco à privacidade, avaliar os riscos e realizar o plano de tratamento de riscos.

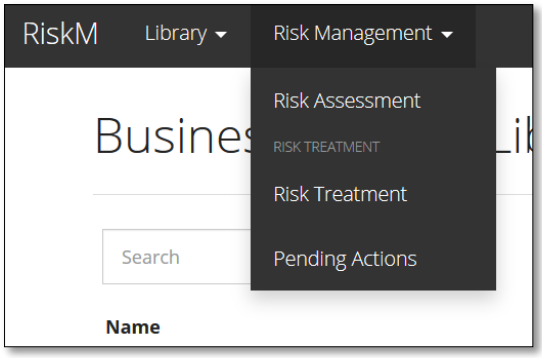

Figura 23 – Menu Gestão do Risco (“Risk Management”) para iniciar a apreciação do risco e ações de tratamento de risco.

Ao despoletar uma apreciação do risco é necessário indicar o processo de negócio a avaliar. Ao realizar a apreciação do risco, surge um ecrã onde podemos observar todos os serviços, servidores e informação associados ao processo de negócio sob avaliação. Neste caso, conforme podemos observar na Figura 24, ao realizar uma avaliação de

risco na privacidade ao processo de negócio FP.20 – Registar Domínios, surge-nos a listagem dos ativos associados. A cada ativo de informação pessoal sob tratamento é possível identificar os riscos associados e efetuar a sua análise e avaliação quanto à sua verosimilhança e impacto na privacidade. É ainda possível visualizar para cada um dos riscos associados, os controlos atualmente implementados e adicionar ou remover controlos conforme necessário.

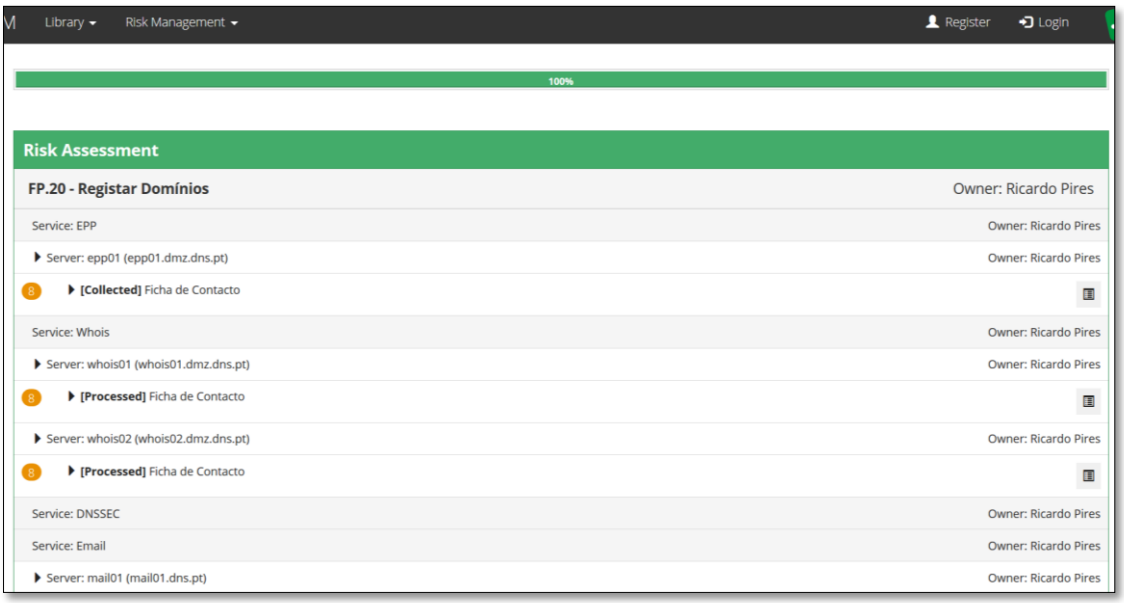

Figura 24 – Menu de apreciação dos riscos na privacidade para o processo FP.20 – Registar Domínios.

Para finalizar, como ilustrado na Figura 25, é possível para cada um dos riscos avaliados com um nível de risco superior ao aceitável identificar ações para os tratar. Neste menu, à semelhança da aplicação atualmente implementada no .PT, identificam-se a causa do problema, o plano de ações para o tratar, o controlo a associar ao tratamento, o custo e o prazo estimado para implementação das ações, a prioridade de implementação das ações e ainda o risco residual estimado.

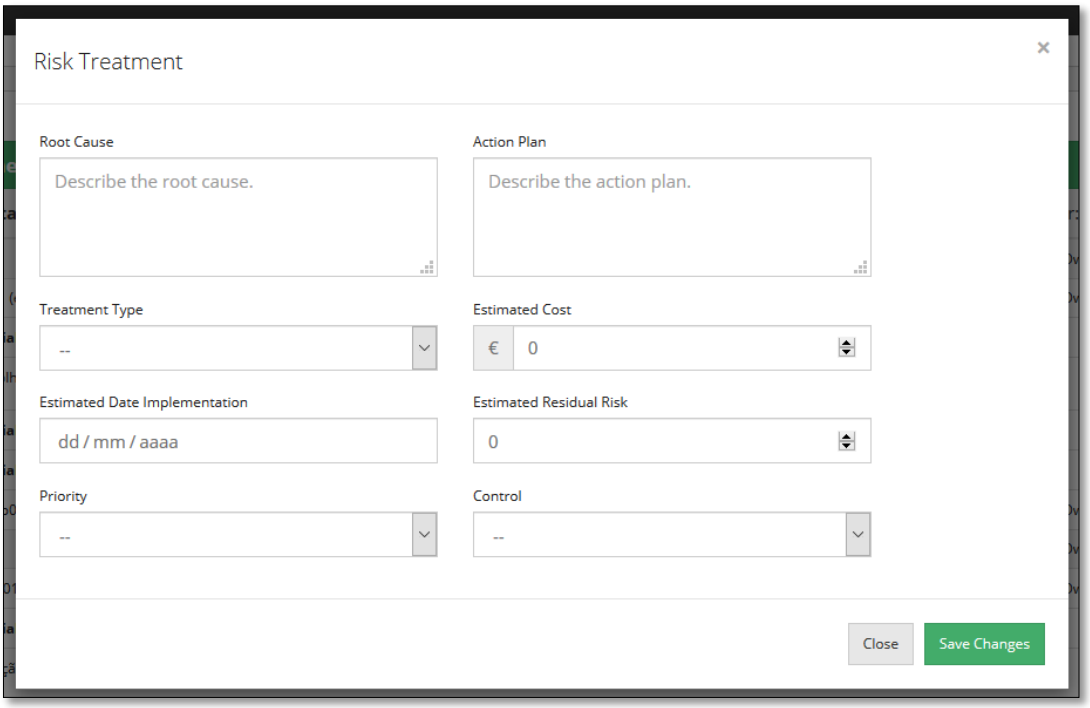

Figura 25 – Menu para definição de ações de tratamento de risco.

Todas as ações provenientes do plano de tratamento de risco passam a ser visíveis no separador de "Pending Actions", ilustrado na Figura 26. Neste menu, podemos ver os riscos identificados com nível superior ao aceitável, o respetivo ativo afetado, a causa do risco e o plano de ações para o tratar. É ainda possível neste menu, quando se conclui o plano de ações, sinalizar o risco como tratado, no botão "Close", fechando desta forma o ciclo de gestão do risco.

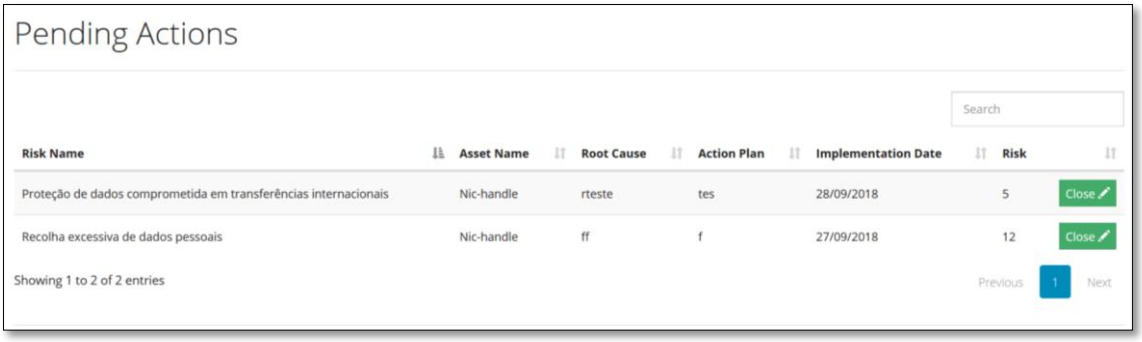

Figura 26 – Menu de ações pendentes do plano de tratamento de risco.

5.3 Resultados da utilização da aplicação

A necessidade de adoção de um modelo para a gestão do risco em segurança da informação e privacidade e do desenvolvimento de uma aplicação que lhe desse suporte surgiu no contexto do .PT, mais propriamente no departamento de gestão e administração, quando surgiram novas regras no tratamento de dados pessoais, o RGPD.

Após o desenvolvimento da aplicação, foi inserida na base de dados da mesma toda a base de processos de negócio, ativos, riscos, controlos e requisitos e respetivas dependências, necessárias para a apreciação dos riscos de privacidade associados ao procedimento PE.47- Registo de nomes de domínio .PT.

O teste da aplicação desenvolvida decorreu com uma vogal do conselho diretivo do .PT e ainda com uma jurista pertencente ao departamento de gestão e administração da organização. Ambas as utilizadoras têm conhecimento sobre a matéria da proteção de dados e ainda com experiência com sistemas de gestão, nomeadamente, o sistema adotado na organização em estudo.

O teste focou-se apenas no procedimento disponível, PE.47, tendo como objetivo validar a adequação da metodologia e do desenho da aplicação. Avaliou-se também se a interface é amigável e se traz vantagens relativamente à aplicação previamente em utilização para a gestão dos riscos no .PT. Testaram-se as funcionalidades de gestão de: ativos, processos de negócio, requisitos, riscos e controlos e, ainda, as funcionalidades respeitantes à apreciação e tratamento do risco na privacidade.

O teste iniciou com a apresentação do modelo e do processo concebido para a gestão dos riscos na privacidade, tendo sido exposta a estrutura hierárquica dos ativos desenvolvida e dos processos de negócio e ainda a relação entre requisitos, riscos e controlos. Foi ainda explicado o processo de gestão dos riscos, incluindo a sua fase de identificação, análise, avaliação e tratamento dos riscos.

As utilizadoras consideraram que o modelo da aplicação em formato de *web service* e a interface apresentada demonstrava vantagens em relação à aplicação anterior, pois permitia um acesso mais facilitado aos diferentes intervenientes e ainda uma interface mais amigável e intuitiva, quer seja na vertente de apreciação e tratamento de riscos, quer seja na gestão da biblioteca dos ativos, processos de negócio, requisitos, riscos e controlos.

Particularmente em relação à funcionalidade de apreciação do risco na privacidade, foi realizado um teste com os referidos elementos do .PT, onde se procedeu à identificação, análise e avaliação dos riscos à privacidade dos elementos de informação tratados no âmbito do procedimento PE.47. Do teste realizado concluiu-se, que o modelo concebido e o respetivo processo de gestão de risco respeitavam as necessidades da organização e os requisitos impostos pelo RGPD e que, de forma sistemática, foi possível identificar situações de risco para a privacidade que deveriam ser mitigadas.

Na apreciação do risco de privacidade no serviço de e-mail, em particular no armazenamento de notificações de contacto ao cliente, e ainda no serviço de Gestão Documental, relativamente ao armazenamento do comprovativo de registo de um nome de domínio, foi identificado um risco de "Impossibilidade de exercício do direito ao apagamento", por não existirem mecanismos que permitiam catalogar, de modo automático, toda a informação respeitante a um titular e desta forma garantir o seu apagamento na totalidade quando solicitado. Este apagamento da informação, quando solicitado, é executado atualmente de forma manual o que pode levar a erros e, desta forma, levar ao incumprimento do requisito.

Relativamente ao risco identificado de "Falta de mecanismos ou políticas de eliminação de dados pessoais (períodos de retenção excessivos)", nos serviços de e-mail e gestão documental, uma vez que não se encontram definidos atualmente períodos de retenção, os dados estão a ser conservados sem um critério.

Tendo em conta os riscos identificados, na fase de tratamento dos riscos, foram identificadas e planeadas as ações a desenvolver para os mitigar. Estes riscos já estão a ser endereçados atualmente pelo .PT, estando já a decorrer as respetivas ações identificadas.

Considera-se assim que a aplicação desenvolvida cumpre com as necessidades da organização para a gestão dos riscos da privacidade, respeitando tanto as novas regras impostas pelo RGPD e o contexto da organização e o processo de gestão de risco atualmente em vigor no .PT.

O modelo conceptualizado, o processo e a aplicação desenvolvida para a gestão do risco em segurança da informação e privacidade trouxeram mais valias à organização, na medida em que, permite à organização numa aplicação mais amigável e intuitiva, comparativamente à anterior, avaliar de forma sistemática os riscos para a

privacidade e ainda identificar, priorizar e acompanhar as ações de tratamento a desenvolver.

Foram ainda assim, apontadas algumas melhorias a realizar futuramente tais como a possibilidade de mostrar informação relativamente às escalas de avaliação no momento da análise dos riscos (informação de suporte).

Capítulo 6

Conclusão e Trabalho Futuro

Este capítulo apresenta as conclusões do trabalho desenvolvido e apresenta alguns desenvolvimentos futuros que podem melhorar o modelo e a aplicação projetada.

6.1 Conclusão

Este trabalho propõe uma abordagem para a gestão do risco em segurança da informação e privacidade, que permite de forma sistemática identificar potenciais riscos ao incumprimento com os requisitos impostos ao tratamento de dados pessoais. A sistematização do processo de gestão dos riscos na privacidade permite à organização, por um lado, identificar potenciais problemas com o cumprimento dos requisitos no tratamento de dados pessoais e desta forma antecipar medidas que tratem o risco. Por outro lado, esta sistematização facilita o acompanhamento e monitorização da implementação das medidas identificadas.

Foi desenhada e implementada ainda uma aplicação para suportar o modelo e o processo de gestão de risco na privacidade no âmbito deste trabalho. A aplicação desenvolvida foi testada na organização em estudo, o .PT, tendo-se concluído que se adequavam tanto o contexto da organização como também respondiam aos requisitos impostos pelo RGPD.

A aplicação da abordagem de gestão do risco desenvolvida permite aos gestores da organização, de forma consciente identificar os potenciais problemas no tratamento de dados pessoais, planear e priorizar as medidas para as tratar. O tratamento dos riscos da privacidade pode, desta forma, evitar o incumprimento com o Regulamento Geral de Proteção de Dados, através da implementação preventiva de controlos e, desta forma, evitar efeitos adversos na componente financeira, com o pagamento das coimas previstas no RGPD, ou mesmo na reputação da organização.

O modelo de gestão de riscos na privacidade foi desenvolvido considerando o contexto da organização do .PT, no entanto, atento às premissas deste modelo, o alinhamento das atividades a processos de negócio, considero que este é passível de poder ser adotado em qualquer outro ramo de negócio onde se efetue tratamento de dados pessoais.

6.2 Trabalho Futuro

Com o desenvolvimento deste modelo e respetiva aplicação para a gestão do risco em segurança da informação e privacidade espera-se ajudar a organização em estudo a identificar potenciais problemas com o tratamento de dados pessoais e a identificar as ações necessárias para os tratar.

Considerando o resultado deste trabalho, existem alguns desenvolvimentos que poderiam acrescentar valor à aplicação desenvolvida e ao modelo e processo de gestão dos riscos na privacidade.

Dos resultados obtidos no decorrer dos testes, considera-se que, relativamente ao processo de gestão dos riscos na privacidade, em particular na fase de avaliação do risco o cálculo do risco poderia ser mais fiável se, a cada controlo fosse associado um fator de mitigação do risco, por exemplo, a implementação do controlo "utilização de palavras-chave fortes" reduziria o risco de "leitura não autorizada" numa quantidade percentual a definir.

Foi ainda sugerido, no momento da avaliação da aplicação, que seria uma mais valia a utilização de mecanismos de segregação dos acessos aos menus das aplicações e das funções associadas a cada um destes. A implementação deste mecanismo iria permitir a criação de utilizadores com diferentes perfis de acesso, e desta forma por exemplo, restringir a gestão dos ativos aos colaboradores do departamento técnico ou ainda permitir que a apreciação do risco fosse apenas iniciada por um membro do departamento de gestão e administração.

Por fim, uma vez que o modelo de gestão do risco concebido, está alinhado com o atual processo de gestão de risco do .PT, é possível integrar as restantes funcionalidades do sistema em vigor no .PT na aplicação desenvolvida, como por exemplo, a gestão dos riscos de segurança, de qualidade e ainda de continuidade de negócio, como também a produção de documentos de suporte relevantes.

Referências

AEPD (2014) *Guía para una Evaluación de Impacto en la Protección de Datos Personales*. Agencia Española de Protección de Datos.

Almeida, J. M. F. D. (2005) *Breve história da Internet*. Universidade do Minho. Disponível em: http://piano.dsi.uminho.pt/museuv/ (Acedido: 26 de Fevereiro de 2018).

CE (Comissão Europeia) (2012) «Proposta para Regulamentação do Parlamento Europeu e do Conselho para a proteção dos indivíduos no que respeita ao processamento de dados pessoais e livre movimento dos mesmos (RGPD)».

CNIL (2012) *Methodology for Privacy Risk Management; How to implement the Data Protection Act*. Commission Nationale de l'Informatique et des Libertés.

CNPD (2018) *Projeto de Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados*. Disponível em: https://www.cnpd.pt/bin/consultapublica/Projeto_regulamento_1-2018.pdf (Acedido: 27 de Agosto de 2018).

Constituição da República Portuguesa (2005). Assembleia da República Portuguesa.

Directiva 95/46/CE, de 24 de Outubro de 1995, art. 2º (1995). Parlamento Europeu e do Conselho da União Europeia.

DNS.PT (2013a) *Estatutos da Associação DNS.PT*. Disponível em: https://www.dns.pt/fotos/editor2/estatutosdns_2016v2.pdf (Acedido: 5 de Abril de 2018).

DNS.PT (2013b) *Plano de Atividades 2013-2016*. Disponível em: https://www.dns.pt/fotos/editor2/links/plano_de_atividades_2013-2016.pdf (Acedido: 12 de Fevereiro de 2018).

DNS.PT (2016) *Plano Estratégico 2016-2019*. Disponível em: https://www.dns.pt/fotos/editor2/plano_estrategico_2016_2019.pdf (Acedido: 16 de Fevereiro de 2018).

DNS.PT (2017a) *Manual de Gestão Integrada do .PT*. Associação DNS.PT.

DNS.PT (2017b) *Metodologia de Gestão de Risco do .PT*. Associação DNS.PT.

DNS.PT (sem data) *O Sistema DNS*. Disponível em: https://www.dns.pt/pt/dominios-2/o-sistema-dns/ (Acedido: 26 de Fevereiro de 2018).

Elgesiem, D. (1996) «Privacy, respect for persons, and risk», em *Philosophical perspectives on computer-mediated communication*. Albany: State University of New York Press, pp. 45–66.

Hull, K. (1992) «Risk analysis techniques in defence procurement», *IEE Colloquium on Risk Analysis Methods and Tools*. London, p. 3/1-317.

ICANN (2013) *Report on the Redelegation of the .PT domain representing Portugal to Associação DNS.PT*. Disponível em: https://www.iana.org/reports/2013/pt-report-20130808.html (Acedido: 12 de Janeiro de 2018).

ICO (2014) *Conducting privacy impact assessments code of practice*. Information Commissioner's Office. Disponível em: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

ICO (sem data) *What we do*. Disponível em: https://ico.org.uk/about-the-ico/ (Acedido: 24 de Fevereiro de 2018).

ISO/IEC (2011a) *ISO/IEC 27005:2011 - Information technology - Security techniques -Information security risk management*.

ISO/IEC (2011b) *ISO/IEC 29100:2011 - Information technology - Security techniques - Privacy framework*. International Organization for Standardization e International Electrotechnical Commission.

ISO/IEC (2013) *NP ISO/IEC 27001:2013 - Tecnologia de informação - Técnicas de Segurança - Sistemas de gestão de segurança da informação - Requisitos*.

ISO (2013) *NP ISO 31000:2009 - Gestão de Risco - Principios e linhas de orientação*. International Organization for Standardization.

ISO (2017) *The ISO Survey of Management System Standard Certifications 2016*. Disponível em: http://www.iso.org/iso/home/standards/certification/iso-survey.htm (Acedido: 16 de Fevereiro de 2018).

Karp, P. (1971) *RFC 226*. Disponível em: https://tools.ietf.org/html/rfc226 (Acedido: 26 de Fevereiro de 2018).

Lei nº 67/98 (1998) «Lei da proteção de dados pessoais», *Diário da República*, 1(247), pp. 5536–5546. Disponível em: https://dre.pt/application/file/239889.

Leiner, B. M., Kahn, R. E., Postel, J., Cerf, V. G., Kleinrock, L., Roberts, L. G., Clark, D. D., Lynch, D. C. e Wolff, S. (2009) «A brief history of the internet», *ACM*

SIGCOMM Computer Communication Review, 39(5), pp. 22–31.

Licklider, J. C. R. e Clark, W. E. (1962) «On-line man-computer communication», *Proceedings of the May 1-3, 1962, spring joint computer conference on - AIEE-IRE '62 (Spring)*, p. 113.

McNamee, D. (1998) *Business Risk Assessment*. 5ª Edição. The Institute of Internal Auditors Research Foundation.

Mockapetris, P. (1983) *RFC 882*. Disponível em: https://tools.ietf.org/html/rfc882 (Acedido: 26 de Fevereiro de 2018).

OCDE (1980) *OECD Privacy Guidelines, The OECD Privacy Framework*. Organização para a Cooperação e Desenvolvimento Económico.

Oetzel, M. C. e Spiekermann, S. (2014) «A systematic methodology for privacy impact assessments: A design science approach», *European Journal of Information Systems*, 23(2), pp. 126–150.

P. Mockapetris (1983) *RFC 883*. Disponível em: https://tools.ietf.org/html/rfc883 (Acedido: 26 de Fevereiro de 2018).

Porto Editora (2018) *Dicionário infopédia da Língua Portuguesa*. Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/risco (Acedido: 24 de Fevereiro de 2018).

Postel, J. (1994) *RFC1591, IETF*. Disponível em: https://www.ietf.org/rfc/rfc1591.txt (Acedido: 16 de Fevereiro de 2018).

Regulamento Geral sobre a Proteção de Dados, 2016/679 (2016). Parlamento Europeu e do Conselho da União Europeia.

Root Server Technical Operations Association (sem data) *Root Servers*. Disponível em: http://root-servers.org (Acedido: 26 de Março de 2018).

Smith, R. e Shao, J. (2007) «Privacy and e-commerce: A consumer-centric perspective», *Electronic Commerce Research*, 7(2), pp. 89–116.

Stewart, B. (1999) «Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies.», *Privacy Law & Policy Reporter 5.8*, pp. 147–149.

Tribunal Europeu dos Direitos Humanos (1950) «Convenção Europeia dos Direitos do Homem», *Convenção para a proteção dos direitos humanos e da liberdades fundamentais*. Conselho da Europa.

Venier, S. (2010) *The respect to privacy in different cultural contexts, EACME Annual Meeting*. Oslo. Disponível em: https://www.prescient-

project.eu/prescient/inhalte/download/VenierEACME2010.pdf (Acedido: 16 de Fevereiro de 2018).

Warren, S. D. e Brandeis, L. D. (1890) «The Right to Privacy», *Harv. L. Rev.*, 4(5), pp. 193–220.

Whitman, M. E. e Mattord, H. J. (2014) *Management of information security*. 4th ed. Course Technology Ptr.

Anexo 1

Aplicação protótipo

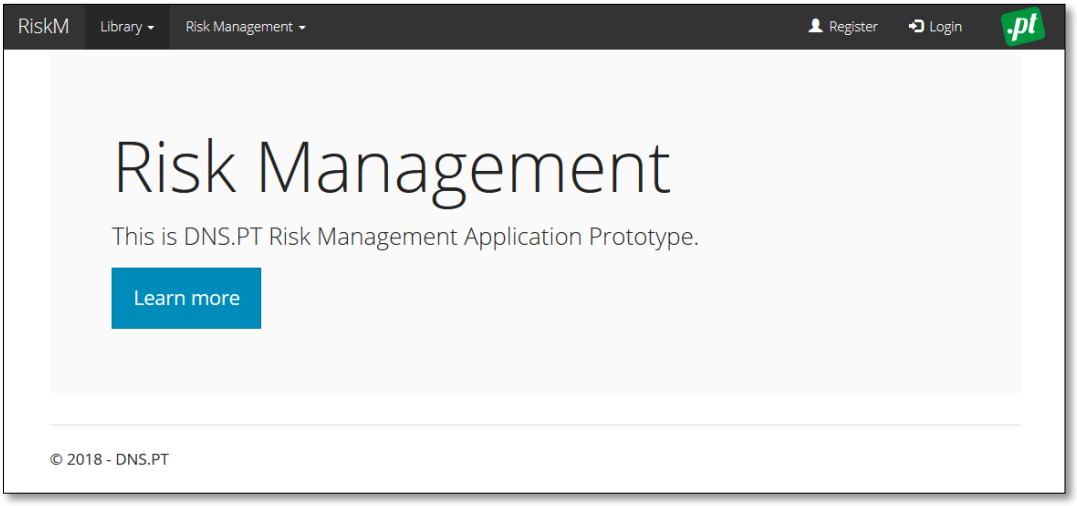

Figura 27 – Aplicação Protótipo - Menu inicial.

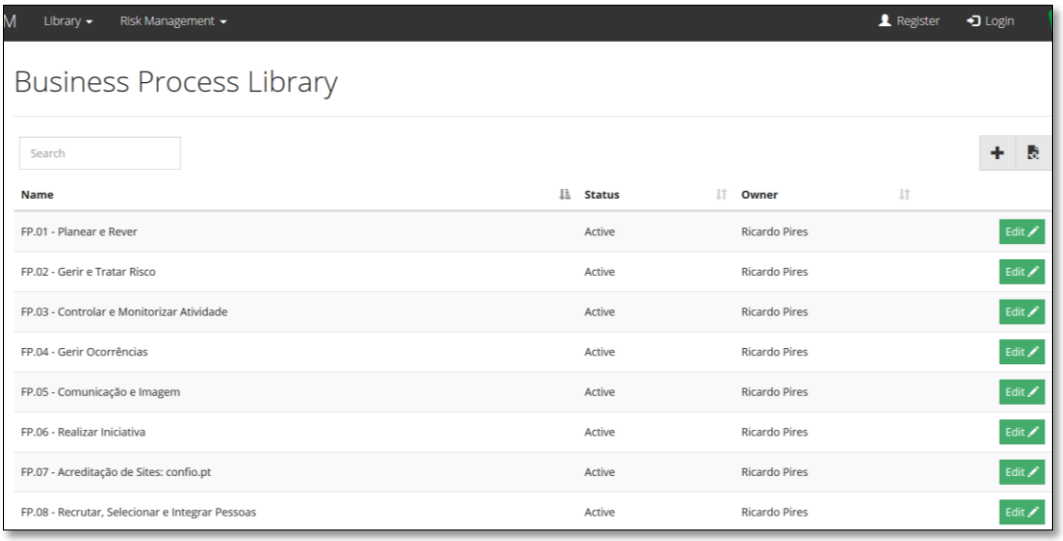

Figura 28 – Aplicação Protótipo - Menu para gestão dos processos de negócio.

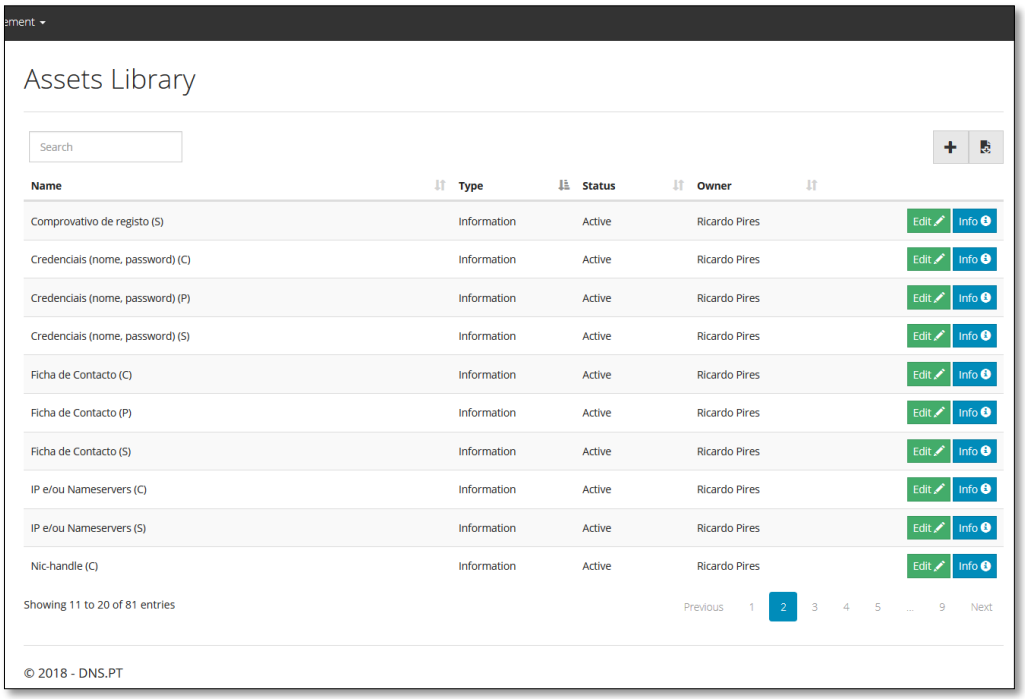

Figura 29 – Aplicação Protótipo - Menu para gestão dos ativos.

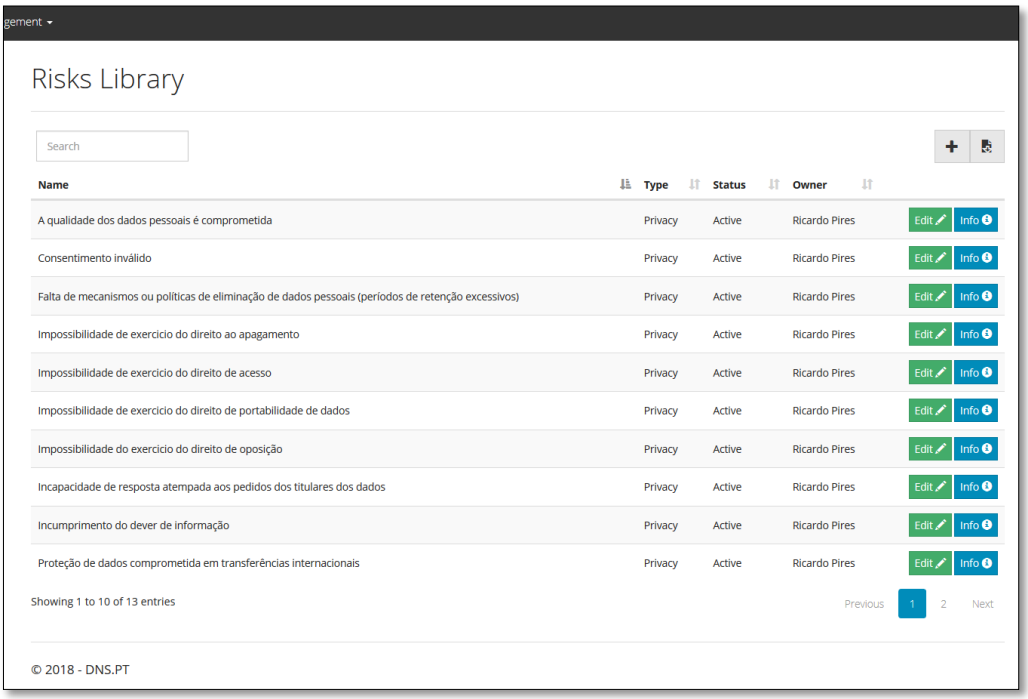

Figura 30 – Aplicação Protótipo - Menu para gestão dos riscos.

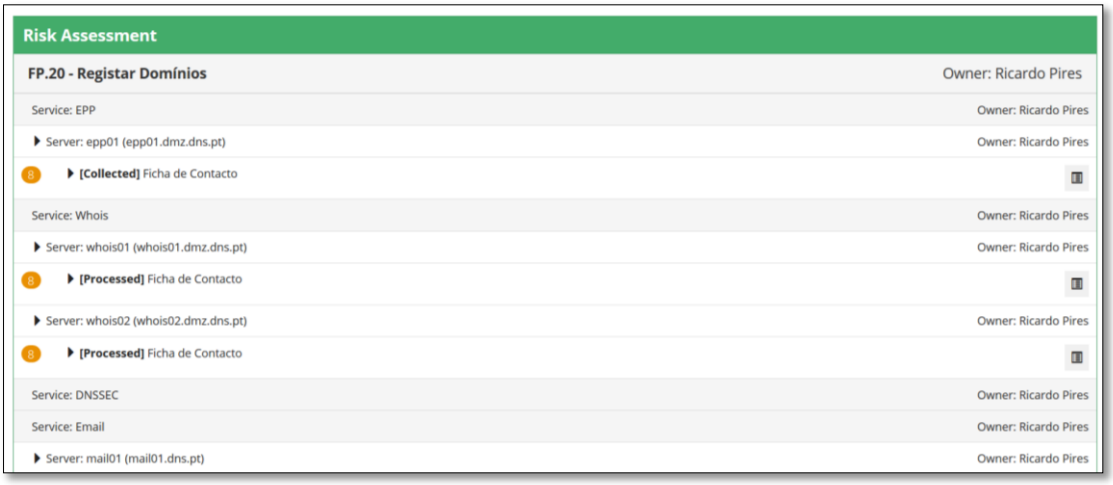

Figura 31 – Aplicação Protótipo - Menu para avaliar os riscos na privacidade.

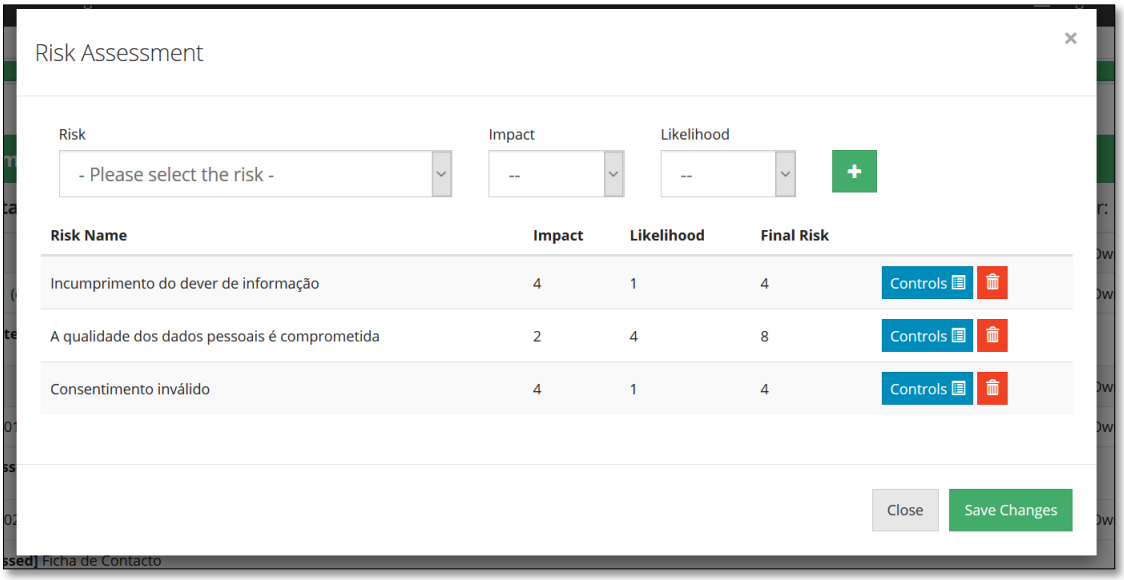

Figura 32 – Aplicação Protótipo - Menu para avaliar os riscos na privacidade.

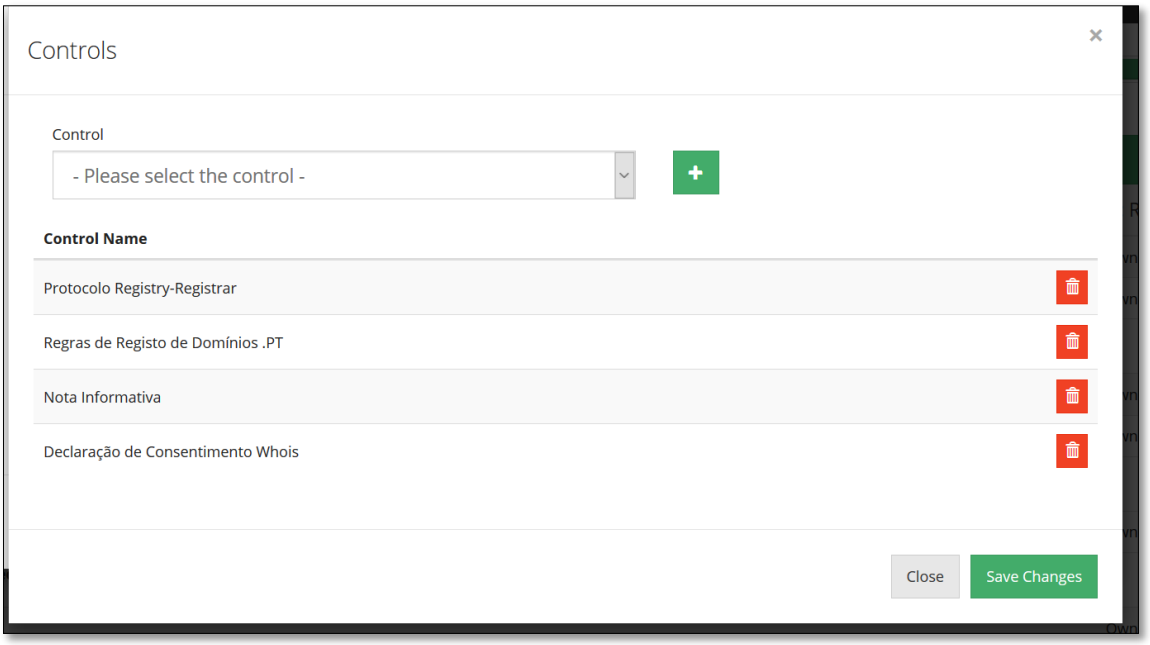

Figura 33 – Aplicação Protótipo - Menu para novos adicionar controlos aos riscos.

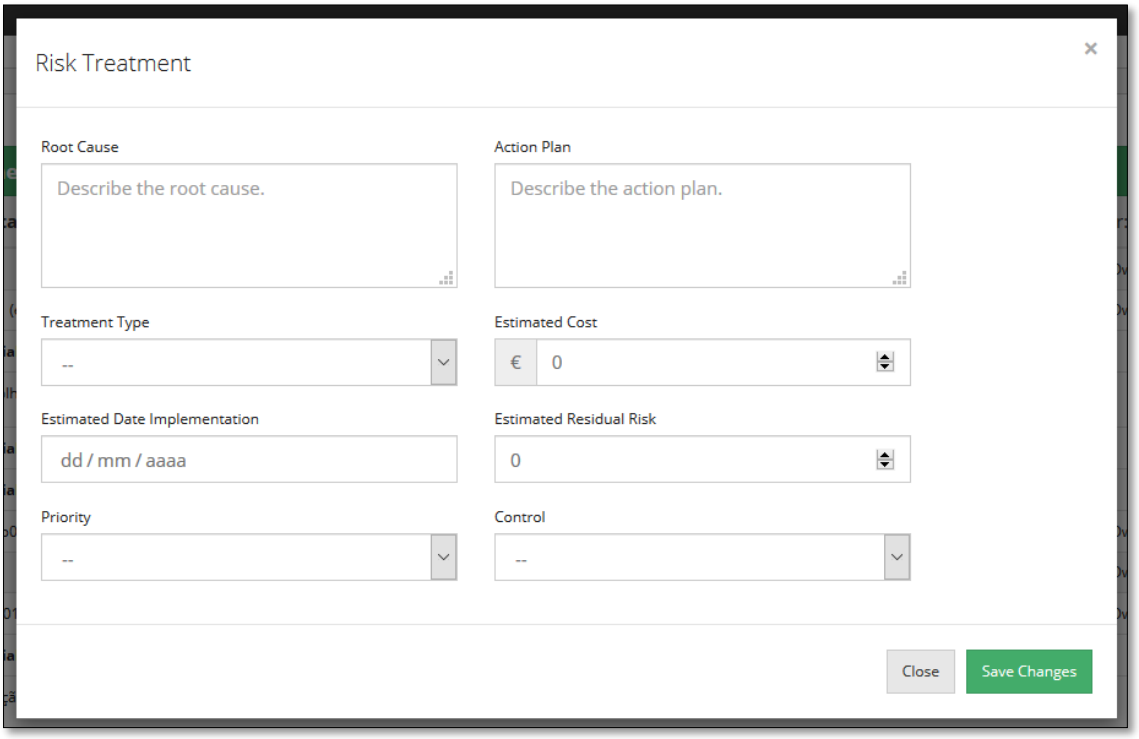

Figura 34 – Aplicação Protótipo – Menu para de tratamento dos riscos.

Figura 35- Aplicação protótipo – Menu para gestão das medidas de tratamento de risco.

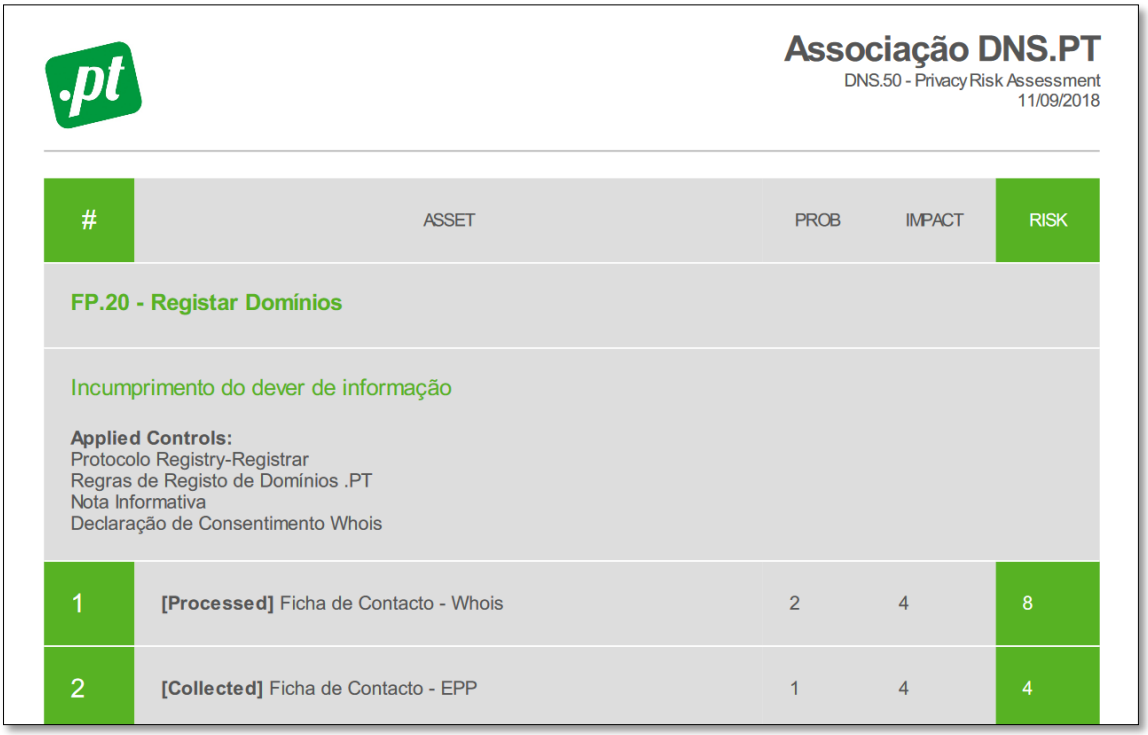

Figura 36 – Aplicação protótipo – Relatório final de avaliação dos riscos.